UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/958,252	07/12/2022	11387982	GMT3707US_QM_0011016	5318

180929 7590 06/22/2022

THALES DIS CPL USA, INC.
Marc BOILLOT
900 South Pine Island Road – Suite 710
PLANTATION, FL 33324

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

INVENTOR(s) (Please see PAIR WEB site http://pair.uspto.gov for additional inventors):

Fabrice DELHOSTE, LA CIOTAT, FRANCE;
Frédéric PAILLART, Gemenos, FRANCE;
Sébastien PETIT, LA CIOTAT, FRANCE;

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

THALES DIS FRANCE SAS, Meudon, FRANCE;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

IR103 (Rev. 10/09)

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/958,252	DELHOSTE et al.
	Examiner	**Art Unit**
	MAYASA A SHAAWAT	2433

CPC							
Symbol						**Type**	**Version**
H04L	/	9	/	0643		F	2013-01-01
H04L	/	9	/	0866		I	2013-01-01
H04L	/	9	/	3231		I	2013-01-01
H04L	/	9	/	3242		I	2013-01-01

CPC Combination Sets								
Symbol						**Type**	**Set**	**Ranking**	**Version**
	/		/						

/MAYASA A. SHAAWAT/ Examiner, Art Unit 2433	01 June 2022	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	10	
/JEFFREY C PWU/ Supervisory Patent Examiner, Art Unit 2433	01 June 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	16	2

U.S. Patent and Trademark Office — Part of Paper No.: 20220601

Thales Exhibit 2001, Page 2 of 339
Okta v. Thales DIS France - IPR2026-00278

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/958,252	DELHOSTE et al.
	Examiner	**Art Unit**
	MAYASA A SHAAWAT	2433

INTERNATIONAL CLASSIFICATION					
CLAIMED					
H04L	/	9	/	06	

NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

/MAYASA A. SHAAWAT/ Examiner, Art Unit 2433	01 June 2022	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	10	
/JEFFREY C PWU/ Supervisory Patent Examiner, Art Unit 2433	01 June 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	16	2

U.S. Patent and Trademark Office — Part of Paper No.: 20220601

Thales Exhibit 2001, Page 3 of 339
Okta v. Thales DIS France - IPR2026-00278

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/958,252	DELHOSTE et al.
	Examiner	**Art Unit**
	MAYASA A SHAAWAT	2433

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	16	10	25												
2	17														
3	18														
4	19														
5	20														
6	21														
7	22														
8	23														
9	24														

/MAYASA A. SHAAWAT/ Examiner, Art Unit 2433	01 June 2022	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	10	
/JEFFREY C PWU/ Supervisory Patent Examiner, Art Unit 2433	01 June 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	16	2

U.S. Patent and Trademark Office — Part of Paper No.: 20220601

Thales Exhibit 2001, Page 4 of 339
Okta v. Thales DIS France - IPR2026-00278

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/958,252	DELHOSTE et al.
	Examiner	**Art Unit**
	MAYASA A SHAAWAT	2433

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/07/2021	04/01/2022							
16	16	✓	=							
17	17	✓	=							
18	18	✓	=							
19	19	✓	=							
20	20	✓	=							
21	21	✓	=							
22	22	✓	=							
23	23	✓	=							
24	24	✓	=							
25	25	✓	=							

Thales Exhibit 2001, Page 5 of 339
Okta v. Thales DIS France - IPR2026-00278

PART B – FEE(S) TRANSMITTAL

Complete and send this form, together with the applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By fax, send to: (571) 273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate " FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Marc BOILLOT

THALES DIS CPL USA Inc
900 South Pine Island Road – Suite 710
Plantation, Florida 33324 – U.S.A.

e-mail: us.intellectualproperty@thalesgroup.com
Phone: 954-658-0418

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

Marc BOILLOT	(Typed or printed name)
/Marc BOILLOT/	(Signature)
May 3 2022	(Date)

APPLICATION NO	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO	CONFIRMATION NO
16/958,252	June 26 2020	Fabrice DELHOSTE	GMT3707US_QM_0011016	5318

TITLE OF INVENTION:

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
Non Provisional	UNDISCOUNTED	$1200	$0.00	$0.00	$1200	07/19/2022

EXAMINER	ART UNIT	CLASS-SUBCLASS

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363)

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ " Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1.

2. Marc BOILLOT - THALES DIS CPL USA, Inc

3.

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: THALES DIS FRANCE SAS

(B) RESIDENCE: (CITY and STATE or COUNTRY): MEUDON, FRANCE

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☑ Corporation or other private group entity ☐ Government

4a. Fees Submitted: ☑ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment (*Please first reapply any previously paid fee shown above*):

☑ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 604092

5. Change of Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29. NOTE: Absent a valid Certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27. NOTE: If the application was previously under micro entity status, checking this box will be taken as a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status. NOTE: Checking this box will be taken as a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Marc BOILLOT/ Date May 3 2022

Typed or printed name Marc BOILLOT Registration No. 56164

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	16958252
Filing Date:	26-Jun-2020
Title of Invention:	METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM
First Named Inventor/Applicant Name:	Fabrice DELHOSTE
Filer:	Marc Andre Boillot/GHEZALI Djouher
Attorney Docket Number:	GMT3707US_QM_0011016

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	1501	1	1200	1200

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1200**

Electronic Acknowledgement Receipt	
EFS ID:	45618184
Application Number:	16958252
International Application Number:	
Confirmation Number:	5318
Title of Invention:	METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM
First Named Inventor/Applicant Name:	Fabrice DELHOSTE
Customer Number:	180929
Filer:	Marc Andre Boillot/GHEZALI Djouher
Filer Authorized By:	Marc Andre Boillot
Attorney Docket Number:	GMT3707US_QM_0011016
Receipt Date:	03-MAY-2022
Filing Date:	26-JUN-2020
Time Stamp:	10:08:22
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1200
RAM confirmation Number	E202253A08441155
Deposit Account	604092
Authorized User	GHEZALI Djouher
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	GMT3707US_Issue_Fee_ptol85.pdf	272214 ee2468a388108d90d138592e9df3a9a754a57e90	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	38569 a2719035821890199340e20f0a899ec907e66084	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	310783		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/958,252	DELHOSTE et al.
	Examiner	**Art Unit**
	MAYASA A SHAAWAT	2433

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/07/2021	04/01/2022							
1	1	-	-							
2	2	-	-							
3	3	-	-							
4	4	-	-							
5	5	-	-							
6	6	-	-							
7	7	-	-							
8	8	-	-							
9	9	-	-							
10	10	-	-							
11	11	-	-							
12	12	-	-							
13	13	-	-							
14	14	-	-							
15	15	-	-							
16	16	✓	=							
17	17	✓	=							
18	18	✓	=							
19	19	✓	=							
20	20	✓	=							
21	21	✓	=							
22	22	✓	=							
23	23	✓	=							
24	24	✓	=							
25	25	✓	=							

Thales Exhibit 2001, Page 12 of 339
Okta v. Thales DIS France - IPR2026-00278

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

180929 7590 04/19/2022

THALES DIS CPL US
THALES DIS USA Inc.
4690 Millennium Drive
Belcamp, MD 21017

EXAMINER
SHAAWAT, MAYASA A.

ART UNIT	PAPER NUMBER
2433	

DATE MAILED: 04/19/2022

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/958,252	06/26/2020	Fabrice DELHOSTE	GMT3707US_QM_0011016	5318

TITLE OF INVENTION: METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1200	$0.00	$0.00	$1200	07/19/2022

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PTOL-85 (Rev. 02/11)

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

180929 7590 04/19/2022
THALES DIS CPL US
THALES DIS USA Inc.
4690 Millennium Drive
Belcamp, MD 21017

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/958,252	06/26/2020	Fabrice DELHOSTE	GMT3707US_QM_0011016	5318

TITLE OF INVENTION: METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1200	$0.00	$0.00	$1200	07/19/2022

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHAAWAT, MAYASA A.	2433	713-189000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Thales Exhibit 2001, Page 14 of 339
Okta v. Thales DIS France - IPR2026-00278

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/958,252	06/26/2020	Fabrice DELHOSTE	GMT3707US_QM_0011016	5318

180929 7590 04/19/2022

THALES DIS CPL US
THALES DIS USA Inc.
4690 Millennium Drive
Belcamp, MD 21017

EXAMINER	
SHAAWAT, MAYASA A.	
ART UNIT	PAPER NUMBER
2433	

DATE MAILED: 04/19/2022

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 02/11)

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 16/958,252	Applicant(s) DELHOSTE et al.	
	Examiner MAYASA A SHAAWAT	Art Unit 2433	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to 02/15/2022.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 16-25 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☑ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☑ All b) ☐ Some* c) ☐ None of the:

   1. ☑ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☑ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☑ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/MAYASA A. SHAAWAT/ Examiner, Art Unit 2433	/JEFFREY C PWU/ Supervisory Patent Examiner, Art Unit 2433

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Response to Arguments

2. Applicant's arguments, see remarks, filed 02/15/2022, with respect to claims 16-25 have been fully considered and are persuasive. The rejections of claims 16-25 has been withdrawn.

EXAMINER'S AMENDMENT

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in an interview with Marc Boillot on 04/05/2022. Claims 16, 23 and 25 have been amended. The new amended limitations have been underlined.

16. (Currently Amended) An authentication method comprising:

- collecting, based on a predetermined authentication policy, at least one context data element;

- constituting a data packet, based on the at least one collected context data element;

- generating a hash, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm

- sending the generated hash;

- generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and

- authenticating successfully or not based on the generated hash distance, as an authentication; **wherein said at least one context data element is a captured image represented as a string of bits with a fixed length for constituting said data packet, and wherein said hash is a byte stream generated from said string of bits representing said captured image for said data packet**.

23. (Currently Amended) A first authentication device, wherein the first authentication device is configured to:

- collect at least one context data element, based on a predetermined authentication policy;

- constitute a data packet, based on the at least one collected context data element;

- generate a hash, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm; and

- send the generated hash to a second authentication device;

wherein said at least one context data element is a captured image represented as a string of bits with a fixed length for constituting said data packet, and wherein said hash is a byte stream generated from said string of bits representing said captured image for said data packet.

25. (Currently Amended) An authentication system, comprising a first authentication device and at least one second authentication device, wherein the first authentication device is configured to:

- collect at least one context data element, based on a predetermined authentication policy;

- constitute a data packet, based on the at least one collected context data element;

- generate a hash, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm; and

- send to the second authentication device, the generated hash;

- and wherein the second authentication device is configured to:

- receive the generated hash from the first device;

- generate a hash distance between the generated hash and a predetermined reference hash; and

- authenticate successfully or not based on the generated hash distance; **wherein said at least one context data element is a captured image represented as a string of bits with a fixed length for constituting said data packet, and wherein said hash is a byte stream generated from said string of bits representing said captured image for said data packet**.

REASONS FOR ALLOWANCE

4. Claims 16-25 are allowed.

5. The following is an examiner's statement of reasons for allowance: in combination of limitations including authenticating successfully or not based on the generated has distance, as an authentication, wherein said at least one context data element is a captured image represented as a string of bits with a fixed length for constituting said data packet in combination with other limitations independent claims 16, 23 and 25.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to **MAYASA SHAAWAT** whose telephone number is (571)272-3939. The examiner can normally be reached on M-F, 8 AM TO 5 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **JEFFREY PWU** can be reached on (571)272-6789. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see https://ppair-my.uspto.gov/pair/PrivatePair. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MAYASA A. SHAAWAT/
Examiner, Art Unit 2433

/JEFFREY C PWU/
Supervisory Patent Examiner, Art Unit 2433

Examiner-Initiated Interview Summary	**Application No.** 16/958,252	**Applicant(s)** DELHOSTE et al.		
	Examiner MAYASA A SHAAWAT	**Art Unit** 2433	**AIA (First Inventor to File) Status** Yes	**Page** 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	**Title**	**Type**
MAYASA A SHAAWAT	Examiner	Telephonic
MARC BOILLOT	Attorney	

Date of Interview: 05 April 2022

Issues Discussed:

Proposed Amendment(s)

Examiner contacted applicant with proposed amendments for claims 16, 23 and 25. Applicant agreed to amendment.

/MAYASA A. SHAAWAT/ Examiner, Art Unit 2433	/JEFFREY C PWU/ Supervisory Patent Examiner, Art Unit 2433

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Notice of References Cited	Application/Control No. 16/958,252	Applicant(s)/Patent Under Reexamination DELHOSTE et al.	
	Examiner MAYASA A SHAAWAT	Art Unit 2433	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20140108800-A1	04-2014	Lawrence; David	H04L9/3297	713/168
*	B	US-20170109514-A1	04-2017	Cheng; Hui	G06F21/316	1/1
*	C	US-20060020796-A1	01-2006	Aura; Tuomas	H04L63/123	713/168
*	D	US-9514753-B2	12-2016	Sharifi; Matthew	G10L25/51	1/1
*	E	US-20080181403-A1	07-2008	SAKAMOTO; YU	H04L9/3236	380/258
*	F	US-20040221153-A1	11-2004	Kim, Chul-min	H04L9/0637	713/150
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/958,252	DELHOSTE et al.
	Examiner	**Art Unit**
	MAYASA A SHAAWAT	2433

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/07/2021	04/01/2022							
	1	-	-							
	2	-	-							
	3	-	-							
	4	-	-							
	5	-	-							
	6	-	-							
	7	-	-							
	8	-	-							
	9	-	-							
	10	-	-							
	11	-	-							
	12	-	-							
	13	-	-							
	14	-	-							
	15	-	-							
	16	✓	=							
	17	✓	=							
	18	✓	=							
	19	✓	=							
	20	✓	=							
	21	✓	=							
	22	✓	=							
	23	✓	=							
	24	✓	=							
	25	✓	=							

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/958,252	DELHOSTE et al.
	Examiner	**Art Unit**
	MAYASA A SHAAWAT	2433

CPC						
Symbol					**Type**	**Version**
H04L	/	9	/	0643	F	2013-01-01
H04L	/	9	/	0866	I	2013-01-01
H04L	/	9	/	3231	I	2013-01-01
H04L	/	9	/	3242	I	2013-01-01

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

/MAYASA A. SHAAWAT/ Examiner, Art Unit 2433	05 April 2022	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	10	
/JEFFREY C PWU/ Supervisory Patent Examiner, Art Unit 2433	07 April 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	16	2

U.S. Patent and Trademark Office — Part of Paper No.: 20220401

Thales Exhibit 2001, Page 27 of 339
Okta v. Thales DIS France - IPR2026-00278

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/958,252	DELHOSTE et al.
	Examiner	**Art Unit**
	MAYASA A SHAAWAT	2433

INTERNATIONAL CLASSIFICATION					
CLAIMED					
H04L	/	9	/	06	

NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

/MAYASA A. SHAAWAT/ Examiner, Art Unit 2433	05 April 2022	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	10	
/JEFFREY C PWU/ Supervisory Patent Examiner, Art Unit 2433	07 April 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	16	2

U.S. Patent and Trademark Office — Part of Paper No.: 20220401

Thales Exhibit 2001, Page 28 of 339
Okta v. Thales DIS France - IPR2026-00278

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/958,252	DELHOSTE et al.
	Examiner	**Art Unit**
	MAYASA A SHAAWAT	2433

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
16	16	25	25												
17	17														
18	18														
19	19														
20	20														
21	21														
22	22														
23	23														
24	24														

/MAYASA A. SHAAWAT/ Examiner, Art Unit 2433	05 April 2022	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	10	
/JEFFREY C PWU/ Supervisory Patent Examiner, Art Unit 2433	07 April 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	16	2

U.S. Patent and Trademark Office Part of Paper No.: 20220401

Thales Exhibit 2001, Page 29 of 339
Okta v. Thales DIS France - IPR2026-00278

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/958,252	DELHOSTE et al.
	Examiner	Art Unit
	MAYASA A SHAAWAT	2433

CPC - Searched*		
Symbol	Date	Examiner
H04L9/0643, H04L9/0866 , H04L9/3231, H04L9/3242	09/08/2021	MAS

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
H04L9/0643, H04L9/0866 , H04L9/3231, H04L9/3242	09/08/2021	MAS
PE2E search	09/07/2021	MAS
inventor and applicant search	09/07/2021	MAS
ip.com search	09/07/2021	MAS
espacenet.com	09/07/2021	MAS
revised PE2E search	04/05/2022	MAS
revised ip.com search	04/05/2022	MAS

/MAYASA A. SHAAWAT/ Examiner, Art Unit 2433	/JEFFREY C PWU/ Supervisory Patent Examiner, Art Unit 2433

Thales Exhibit 2001, Page 30 of 339
Okta v. Thales DIS France - IPR2026-00278

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/958,252	DELHOSTE et al.
	Examiner	Art Unit
	MAYASA A SHAAWAT	2433

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
	claims texted search	04/05/2022	MAS

/MAYASA A. SHAAWAT/ Examiner, Art Unit 2433	/JEFFREY C PWU/ Supervisory Patent Examiner, Art Unit 2433

Thales Exhibit 2001, Page 31 of 339
Okta v. Thales DIS France - IPR2026-00278

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	76	((("THALES") near3 ("DIS") near3 ("FRANCE") near3 ("SA"))).AS,AANM.	(USPAT)	OR	ON	ON	2021/09/07 12:14 PM
L2	5	((("DELHOSTE") near3 ("Fabrice")) OR (("PAILLART") near3 ("Frdric")) OR (("PETIT") near3 ("Sbastien"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/07 12:14 PM
L3	165	(L1 L2) AND authentication	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/07 12:24 PM
L4	2	((authentication ADJ policy) SAME data SAME element SAME hash WITH algorithm)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/07 12:27 PM
L5	0	((authentication OR validat$ OR authorize) SAME (data ADJ packet) SAME (collected OR collection) WITH context SAME hash SAME algorith)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 09:17 AM
L6	2	((authentication OR validat$ OR authorize) SAME (data ADJ packet) SAME (collected OR collection) WITH context SAME hash)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 09:17 AM
L7	0	((authentication OR validat$ OR authorize) SAME (data ADJ packet) SAME (collected OR collection) WITH context SAME (hash ADJ algorithm))	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 09:21 AM
L8	7	((authentication OR validat$ OR authorize) SAME (data ADJ packet) SAME (collected OR collection) WITH context)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 09:28 AM
L9	2	((authentication OR validat$ OR authorize) SAME (data ADJ	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 09:29 AM

		packet) SAME (collected OR collection) WITH context) AND (H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.					
L10	29635	(H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 09:31 AM
L11	403	(authentication SAME (data ADJ packet)) AND (H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 09:55 AM
L12	1	(weighting SAME (authentication ADJ policy) SAME context WITH (data ADJ element)) AND (H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 10:30 AM
L13	0	((data ADJ packet) WITH ciphering WITH (hash OR HMAC) SAME (authentication ADJ code) SAME derive) AND (H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 04:48 PM
L14	1	((data ADJ packet) WITH ciphering WITH (hash OR HMAC) SAME (authentication ADJ code)) AND (H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 04:48 PM
L15	1	((data ADJ packet) WITH ciphering WITH (hash OR HMAC) SAME (authentication ADJ code))	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 04:48 PM
L16	6	((data ADJ packet) WITH cipher$ WITH (hash OR HMAC) SAME (authentication ADJ code))	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 04:49 PM

L17	1	((data ADJ packet) WITH (hash OR HMAC) WITH distance SAME authentication WITH successfully)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/09 12:36 PM
L18	1	((data ADJ packet) WITH (hash OR HMAC) WITH (distance OR length OR range) SAME authentication WITH successfully)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/09 12:39 PM
L19	102	((("THALES") near3 ("DIS") near3 ("FRANCE") near3 ("SA"))).AS,AANM.	(USPAT)	OR	ON	ON	2022/04/04 06:47 PM
L20	6	((("DELHOSTE") near3 ("Fabrice")) OR (("PAILLART") near3 ("Frdric")) OR (("PETIT") near3 ("Sbastien"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM
L21	204	(L1 L2) AND authentication	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM
L22	2	((authentication ADJ policy) SAME data SAME element SAME hash WITH algorithm)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM
L23	0	((authentication OR validat$ OR authorize) SAME (data ADJ packet) SAME (collected OR collection) WITH context SAME hash SAME algorith)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM
L24	2	((authentication OR validat$ OR authorize) SAME (data ADJ packet) SAME (collected OR collection) WITH context SAME hash)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM
L25	0	((authentication OR validat$ OR authorize) SAME (data ADJ packet) SAME (collected OR collection) WITH context SAME (hash ADJ algorithm))	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM
L26	7	((authentication OR validat$ OR authorize) SAME (data ADJ packet) SAME	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM

		(collected OR collection) WITH context)					
L27	2	((authentication OR validat$ OR authorize) SAME (data ADJ packet) SAME (collected OR collection) WITH context) AND (H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM
L28	33088	(H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM
L29	457	(authentication SAME (data ADJ packet)) AND (H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM
L30	1	(weighting SAME (authentication ADJ policy) SAME context WITH (data ADJ element)) AND (H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM
L31	0	((data ADJ packet) WITH ciphering WITH (hash OR HMAC) SAME (authentication ADJ code) SAME derive) AND (H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM
L32	1	((data ADJ packet) WITH ciphering WITH (hash OR HMAC) SAME (authentication ADJ code)) AND (H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM
L33	1	((data ADJ packet) WITH ciphering WITH (hash OR HMAC) SAME (authentication	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM

		ADJ code))					
L34	7	((data ADJ packet) WITH cipher$ WITH (hash OR HMAC) SAME (authentication ADJ code))	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM
L35	1	((data ADJ packet) WITH (hash OR HMAC) WITH distance SAME authentication WITH successfully)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM
L36	1	((data ADJ packet) WITH (hash OR HMAC) WITH (distance OR length OR range) SAME authentication WITH successfully)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/04/04 06:47 PM
L37	7	((authentication ADJ policy) SAME collect$ WITH (context ADJ data) SAME hash WITH algorithm)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/05 02:40 PM
L38	0	((authentication ADJ policy) SAME collect$ WITH captured WITH image SAME (string ADJ bits) SAME hash WITH algorithm)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/05 02:49 PM
L39	0	((authentication ADJ policy) SAME collect$ SAME captured SAME image SAME (string ADJ bits) SAME hash SAME algorithm)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/05 02:50 PM
L40	9	(hash SAME distance WITH (reference ADJ hash) WITH authenticat$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/05 03:00 PM
L41	0	(hash SAME distance WITH (reference ADJ hash) WITH authenticat$ SAME algorithm SAME image SAME string WITH bits)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO;	OR	ON	ON	2022/04/05 03:02 PM

			JPO; DERWENT; IBM_TDB)				
L42	0	(hash SAME distance SAME (reference ADJ hash) SAME authenticat$ SAME algorithm SAME image SAME string SAME bits)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/05 03:03 PM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N1	0	((authentication ADJ policy) SAME collect$ SAME captured SAME image SAME (string ADJ bits) SAME hash SAME algorithm).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/05 02:50 PM
N3	0	(hash SAME distance SAME (reference ADJ hash) SAME authenticat$ SAME algorithm SAME image SAME string SAME bits).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/05 03:05 PM

Bibliographic Data

Application No: 16/958,252

Foreign Priority claimed: (●) Yes ( ) No

35 USC 119 (a-d) conditions met: [✓] Yes [ ] No [ ] Met After Allowance

Verified and Acknowledged: /MAYASA A. SHAAWAT/ Examiner's Signature [ ] Initials

Title: METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
06/26/2020	713	2433	GMT3707US_QM_0011016
RULE			

APPLICANTS

THALES DIS FRANCE SAS, Meudon, FRANCE

INVENTORS

Fabrice DELHOSTE, LA CIOTAT, FRANCE

Frédéric PAILLART, Gemenos, FRANCE

Sébastien PETIT, LA CIOTAT, FRANCE

CONTINUING DATA

This application is a 371 of PCT/EP2018/081759 11/19/2018

FOREIGN APPLICATIONS

EPO EP17306977.4 12/29/2017

IF REQUIRED, FOREIGN LICENSE GRANTED**

07/15/2020

STATE OR COUNTRY

FRANCE

ADDRESS

THALES DIS CPL US
THALES DIS USA Inc.
4690 Millennium Drive
Belcamp, MD 21017
UNITED STATES

FILING FEE RECEIVED

$2,180

Discover Map wherein said at least one context data element i... TIC

The invention relates to an authentication method. The method comprises: - collecting 24, based on a predetermined authentication policy, at least one context data element; - constituting 28, based on the at least one collected context data element, a data packet; - generating 216, by using a...

THALES DIS FRANCE SA

EP3506138A1 | EPO Applications | 2019-07-03 | 4

Authentication method, device and system

The invention relates to an authentication method. The method comprises: - collecting (24), based on a predetermined authentication policy, at least one context data element; - constituting (28), based on the at least one collected context data element, a data packet; - generating (216), by using a...

GEMALTO SA

WO2019129422A1 | WIPO Applications | 2019-07-04 | 4

Authentication method, device and system

The invention relates to an authentication method. The method comprises: - collecting (24), based on a predetermined authentication policy, at least one context data element, - constituting (28), based on the at least one collected context data element, a data packet; - generating (216), by using a...

THALES DIS FRANCE SA [+1]

EP3732600A1 | EPO Applications | 2020-11-04 | 4

Staged data compression, including block-level long-range compression, for data streams in a communications system

HUGHES NETWORK SYS LLC

EP2778987B1 | EPO Patents | 2020-05-13 | 4

System and method for string filtering

A computer-based method for scanning data using string filtering includes compressing a data string using a hashing algorithm to obtain a data-string signature, and then determining that the data-string signature matches a known data-string signatures stored in a lookup table if the signature is...

BOEING CO

US7366910 | US Patents | 2008-04-29 | 4

System and method for string filtering

A computer-based method for scanning data using string filtering includes compressing a data string using a hashing algorithm to obtain a data-string signature, and then determining that the data-string signature matches a known data-string signatures stored in a lookup table if the signature is...

BOEING CO

US20030018531 | US Applications | 2003-02-13 | 4

Relevance

Publication Date

1991

First Our Assignees by Relevanc

THALES DIS FRANCE SAS (1)
THALES DIS FRANCE SA (4)
GEMALTO SA (1)
HUGHES NETWORK SYS ... (31)
BOEING CO (8)
TELEFON AB LM ERICSS... (11)
FUNGIBLE INC (31)
CISCO TECH INC (54)

Charts based on top 1500 results

More V

Result 5

Thales Exhibit 2001, Page 39 of 339
Okta v. Thales DIS France - IPR2026-00278

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
16/958,252	06/26/2020	2433	2180	GMT3707US_QM_0011016	10	4

CONFIRMATION NO. 5318

CORRECTED FILING RECEIPT

180929
THALES DIS CPL US
THALES DIS USA Inc.
4690 Millennium Drive
Belcamp, MD 21017

OC000000131944900

Date Mailed: 02/24/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Fabrice DELHOSTE, LA CIOTAT, FRANCE;
Frédéric PAILLART, Gemenos, FRANCE;
Sébastien PETIT, LA CIOTAT, FRANCE;

Applicant(s)

THALES DIS FRANCE SAS, Meudon, FRANCE;

Assignment For Published Patent Application

THALES DIS FRANCE SAS, Meudon, FRANCE

Power of Attorney: The patent practitioners associated with Customer Number 180929

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/EP2018/081759 11/19/2018

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)
EUROPEAN PATENT OFFICE (EPO) 17306977.4 12/29/2017

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 07/15/2020
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 16/958,252**
Projected Publication Date: Not Applicable
Non-Publication Request: No
Early Publication Request: No
Title

METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM

Preliminary Class

713

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/958,252	06/26/2020	Fabrice DELHOSTE	GMT3707US_QM_0011016

CONFIRMATION NO. 5318

180929
THALES DIS CPL US
THALES DIS USA Inc.
4690 Millennium Drive
Belcamp, MD 21017

POA ACCEPTANCE LETTER

OC000000131944619

Date Mailed: 02/24/2022

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/17/2022.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/sleutchit/

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	16/958,252
Filing Date	November 19 2018
First Named Inventor	Fabrice DELHOSTE
Title	METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM
Art Unit	2433
Examiner Name	SHAAWAT, MAYASA A.
Attorney Docket Number	GMT3707US_MQ

SIGNATURE of Applicant or Patent Practitioner

Signature	/Marc BOILLOT/	Date (Optional)	February 16 2022
Name	Marc BOILLOT	Registration Number	56164
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)	THALES DIS FRANCE SAS		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/80 (07-17)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no person is required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

[X] Practitioners associated with Customer Number: 180929

OR

[X] Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number
Marc BOILLOT	56164

Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

[ ] The address associated with Customer Number:

OR

[ ]

Firm or individual name		
Address		
City	State	Zip
Country		
Telephone	Email	

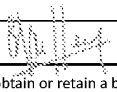
Assignee name and address: THALES DIS FRANCE SAS - 6, rue de la Verrerie - 92190 MEUDON-FRANCE

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of the practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee.

Signature	Date January 18 2022
Name Benoît JOUFFREY	Telephone
Title Chief Technical Officer (CTO)	



This collection of information is required by 37 CFR 1.31, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public, which is to update (and by the USPTO to process) the file of a patent or reexamination proceeding. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 18 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	45009904
Application Number:	16958252
International Application Number:	
Confirmation Number:	5318
Title of Invention:	AUTHENTICATION METHOD, DEVICE AND SYSTEM
First Named Inventor/Applicant Name:	Fabrice DELHOSTE
Customer Number:	180929
Filer:	Marc Andre Boillot
Filer Authorized By:	
Attorney Docket Number:	GMT3707US_QM_0011016
Receipt Date:	17-FEB-2022
Filing Date:	26-JUN-2020
Time Stamp:	08:02:26
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	GMT3707US_Corrected_ADS1.pdf	152783 d362eb80b3ab2f1ee6de967bf31aeb01eb68dc5e	no	9

Warnings:

Information:					
This is not an USPTO supplied ADS fillable form					
2	Assignee showing of ownership per 37 CFR 3.73	GMT3707US_STATE_37CFR.pdf	114176 1603b0f7f16056dae75394988522ba7ee5353130	no	3
Warnings:					
Information:					
3	Power of Attorney	GMT3707US_APPL_GEN_POA.pdf	358029 28dba15e61d4058e6c9d0cb8979a321f9eec4b21	no	3
Warnings:					
Information:					
		Total Files Size (in bytes):	624988		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	~~1032326-001016~~ GMT3707US_QM
	Application Number	16/958,252
Title of Invention	~~AUTHENTICATION METHOD, DEVICE AND SYSTEM~~ METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Fabrice		DELHOSTE	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	~~Gemenos~~ LA CIOTAT	Country of Residence	FR

Mailing Address of Inventor:

Address 1	~~c/o GEMALTO SA, Service Brevets~~ THALES DIS FRANCE SAS – IP Department
Address 2	~~525 avenue du Pic de Bertagne CS12023~~ Avenue du Jujubier – ZI Athélia IV

City	~~Gemenos~~ LA CIOTAT	State/Province	
Postal Code	~~13881~~ 13705	**Country**	FR

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Frédéric		PAILLART	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Gemenos	Country of Residence	FR

Mailing Address of Inventor:

Address 1	~~c/o GEMALTO SA, Service Brevets~~ THALES DIS FRANCE SAS – IP Department
Address 2	~~525 avenue du Pic de Bertagne CS12023~~ Avenue du Jujubier – ZI Athélia IV

City	~~Gemenos~~ LA CIOTAT	State/Province	
Postal Code	~~13881~~13705	**Country**	FR

Inventor 3 Remove

Legal Name

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	~~1032326-001016~~ GMT3707US_QM
	Application Number	16/958,252
Title of Invention	~~AUTHENTICATION METHOD, DEVICE AND SYSTEM~~ METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM	

Prefix	Given Name	Middle Name	Family Name	Suffix
	Sébastien		PETIT	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	~~Gemenos~~ LA CIOTAT	Country of Residence [i]	FR

Mailing Address of Inventor:

Address 1	~~c/o GEMALTO SA, Service Brevets~~ THALES DIS FRANCE SAS – IP Department		
Address 2	~~525 avenue du Pic de Bertagne CS12023~~ Avenue du Jujubier – ZI Athélia IV		
City	~~Gemenos~~ LA CIOTAT	State/Province	
Postal Code	~~1388~~13705	Country [i]	FR

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	~~21839~~180929		
Email Address	us.intellectualproperty@thalesgroup.com	Add Email	Remove Email
Email Address	marc.boillot@thalesgroup.com	Add Email	Remove Email

Application Information:

Title of the Invention	~~AUTHENTICATION METHOD, DEVICE AND SYSTEM~~ METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM		
Attorney Docket Number	~~1032326-001016~~ GMT3707US_QM	Small Entity Status Claimed	
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	2	Suggested Figure for Publication (if any)	2

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a). [i]

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	~~1032326-001016~~ GMT3707US_QM
	Application Number	16/958,252
Title of Invention	~~AUTHENTICATION METHOD, DEVICE AND SYSTEM~~ METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

	◉		
Please Select One:	Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	~~21839~~180929		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	a 371 of international	PCT/EP2018/081759	2018-11-19

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	~~1032326-001016~~ GMT3707US_QM
	Application Number	16/958,252
Title of Invention	~~AUTHENTICATION METHOD, DEVICE AND SYSTEM~~ METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM	

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Remove Access Code[i] (if applicable)
17306977.4	EP	2017-12-29	
Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.			Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	~~1032326-001016~~ GMT3707US_QM
	Application Number	16/958,252
Title of Invention	~~AUTHENTICATION METHOD, DEVICE AND SYSTEM~~ METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	~~1032326-001016~~ GMT3707US_QM
	Application Number	16/958,252
Title of Invention	~~AUTHENTICATION METHOD, DEVICE AND SYSTEM~~ METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◉ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	~~THALES DIS FRANCE SA~~THALES DIS FRANCE SAS		
Mailing Address Information For Applicant:			
Address 1	6, rue de la Verrerie		
Address 2			
City	Meudon	**State/Province**	
Country FR		Postal Code	92190
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	~~1032326-001016~~ GMT3707US_QM
	Application Number	16/958,252

Title of Invention	~~AUTHENTICATION METHOD, DEVICE AND SYSTEM~~ METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☒

Organization Name	~~THALES DIS FRANCE SA~~THALES DIS FRANCE SAS

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1	6, rue de la Verrerie		
Address 2			
City	Meudon	**State/Province**	
Country i	FR	Postal Code	92190
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Marc BOILLOT/			Date (YYYY-MM-DD)	2022-02-16
First Name	Marc	Last Name	BOILLOT	Registration Number	56164

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	~~1032326-001016~~ GMT3707US_QM
	Application Number	16/958,252
Title of Invention	~~AUTHENTICATION METHOD, DEVICE AND SYSTEM~~ METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1 The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3 A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent CooperationTreaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: THALES DIS FRANCE SAS

Application No./Patent No.: 16/958,252 Filed/Issue Date: _____

Titled: METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATIOI

THALES DIS FRANCE SAS, a Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Fabrice Delhoste, Frederic Paillart,Sebastien PETIT To: THALES DIS FRANCE SA

   The document was recorded in the United States Patent and Trademark Office at

   Reel 054960, Frame 0332, or for which a copy thereof is attached.

2. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at

   Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: THALES DIS FRANCE SA To: THALES DIS FRANCE SAS

The document was recorded in the United States Patent and Trademark Office at
Reel 058884, Frame 0238, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Marc BOILLOT	February 7 2022
Signature	Date
/Marc BOILLOT/	N°56164
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal				
Application Number:	16958252			
Filing Date:	26-Jun-2020			
Title of Invention:	AUTHENTICATION METHOD, DEVICE AND SYSTEM			
First Named Inventor/Applicant Name:	Fabrice DELHOSTE			
Filer:	Marc Andre Boillot			
Attorney Docket Number:	GMT3707US_QM_0011016			
Filed as Large Entity				
Filing Fees for U.S. National Stage under 35 USC 371				
Description	**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	1252	1	640	640
Miscellaneous:				
		Total in USD ($)		**640**

Electronic Acknowledgement Receipt	
EFS ID:	44999777
Application Number:	16958252
International Application Number:	
Confirmation Number:	5318
Title of Invention:	AUTHENTICATION METHOD, DEVICE AND SYSTEM
First Named Inventor/Applicant Name:	Fabrice DELHOSTE
Customer Number:	180929
Filer:	Marc Andre Boillot
Filer Authorized By:	
Attorney Docket Number:	GMT3707US_QM_0011016
Receipt Date:	15-FEB-2022
Filing Date:	26-JUN-2020
Time Stamp:	13:30:48
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$640
RAM confirmation Number	E20222ED31161449
Deposit Account	604092
Authorized User	Marc Boillot
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Drawings-only black and white line drawings	GMT3707_OA1_Drawing_Corrected.pdf	25574 621f35cf38c618670424c63b120bc50ff5b732ab	no	1
Warnings:					
Information:					
2		GMT3707_OA1_Response.pdf	83964 bbb6d673648b1c64136da4b4fdfefe99d7c0271e	yes	12

Multipart Description/PDF files in .zip description

Document Description	Start	End
Transmittal Letter	1	1
Amendment/Request for Reconsideration-After Non-Final Rejection	2	12

Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	38770 a159462fe4b42a367216e7cd0dcac8bdcf50c5a9	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	148308		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

REPLACEMENT SHEET

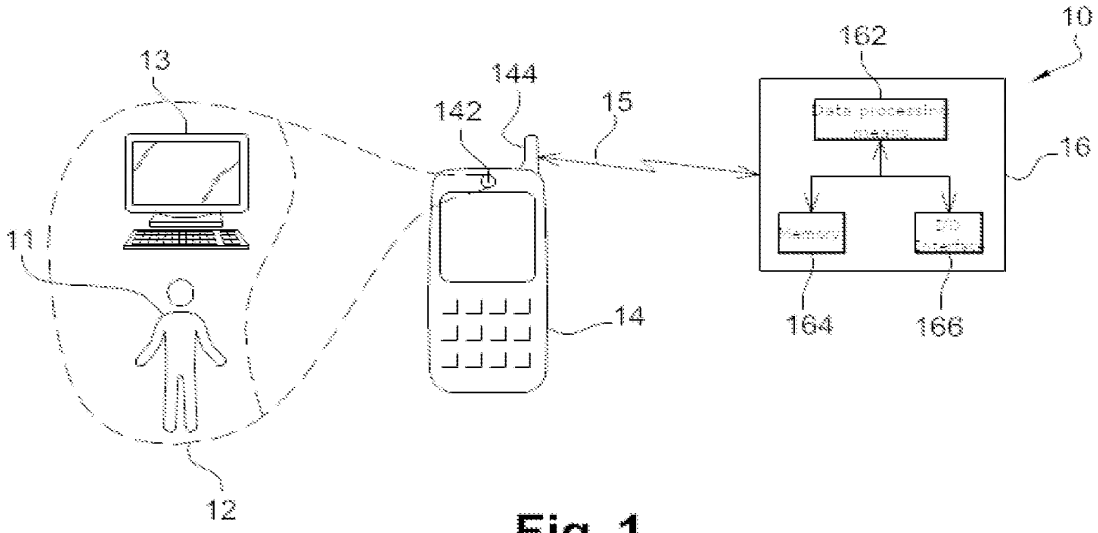


Fig. 1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

U.S. Appln. No.	:	16/958,252	Confirmation No. **5318**
Applicant	:	Fabrice DELHOSTE	
Filed	:	06/26/2020	
TC/A.U.	:	2433	
Examiner	:	Shaawat, Mayasa A.	
Thales Docket No.	:	GMT3707US-WO-MQ-MB	

RESPONSE TO OFFICE ACTION

MAIL STOP Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Date: February 15, 2022

Applicant provides the present Amendment to address the issues raised in the **Non-Final** Office Action mailed September 16, 2021 (hereinafter "Office Action"). Please amend this application as follows and reconsider the rejections of the claims for at least the reasons presented in the following remarks.

The non-statutory 3-month deadline ended December 16, 2021. This response is however being filed within 5 months from the mailing date. Accordingly, a two-month extension fee is believed due. Please charge that fee to Deposit Account No. **60-4092.**

Any additional fees believed to be due in connection with this paper may be charged to that same deposit account.

Amendments to the Specification begin on page **2** of this submission.
Amendments to the Drawings begin on page **3** of this submission.
Remarks/Arguments begin on page **4** of this submission.

Amendments to the Specification:

Per CFR 1.121(b)(1), Applicant hereby amends the specification of the application by "Amendment to delete, replace, or add a paragraph", by submitting instructions to:

On Page 1 of the specification, please delete the title "AUTHENTICATION METHOD, DEVICE AND SYSTEM" and,

by way of the replacement paragraph with markings below to show all the changes relative to the previous version of the paragraph "~~AUTHENTICATION METHOD, DEVICE AND SYSTEM~~ METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM",

please replace with the full text of the added paragraph without any underlining:

"METHOD FOR AUTHENTICATING A HASH OF A DATA PACKET FROM COLLECTED CONTEXT DATA BASED ON A HASH DISTANCE GENERATION STEP, FIRST AUTHENTICATION DEVICE, SECOND AUTHENTICATION DEVICE, AND AUTHENTICATION SYSTEM"

Amendments to the Drawings:

Per MPEP 1.121(d), Applicant hereby amends the drawings, by submitting:

i) replacement drawing, and

ii) an explanation of the changes.

RE i)

Changes to the replacement drawing is in compliance with CFR § 1.84, and are submitted on a replacement sheet of drawings accompanying this document; in the top margin of each labeled "Replacement Sheet".

RE ii)

Replacement sheet for FIG. 1, adds textual descriptors to elements 162, 164, and 166.

The basis for these amendments can be found on page 13, lines 26-27 of the PCT application where it is set forth:

"The server 16 includes one or several CPU(s), (micro)processor(s) and/or (micro)controller(s) 162, as data processing means, one or several memories 164, as data storing means, and one or several I/O interfaces 166 that are internally together connected."

No new matter has been added.

Thales Exhibit 2001, Page 70 of 339
Okta v. Thales DIS France - IPR2026-00278

REMARKS/ARGUMENTS

This communication is a full and timely response to the Office Action dated September 16, 2021. Applicant appreciates the detailed examination evidenced by the Office Action.

Applicant also appreciates the return phone call on February 10, 2022 regarding the objection to the drawings and what would constitute an acceptable correction to Figure 1.

Reconsideration and allowance of the present application are respectfully requested in view of the foregoing Amendments and following Remarks.

STATUS OF CLAIMS

Claims 1-15 were previously cancelled by way of a preliminary amendment.

Claims 16-25 remain pending, of which claims 16, 23, 24 and 25 are the independent claims

Claims 16, 20 and 25 were rejected under 35 U.S.C. 103 as being unpatentable over Lawrence (US 2014/0108800 Al), Cheng (US 2017/109514 Al) and Aura (US 2006/0020796 Al) in view of Sakamoto (US 2008/0181403) - see paragraph 6, on pg 4 of the Office Action,

Claims 17 was rejected under 35 U.S.C. 103 as being unpatentable over Lawrence (US 2014/0108800 Al), Cheng (US 2017/109514 Al), Aura (US 2006/0020796 Al) and Sakamoto (US 2008/0181403 Al) in view of Sharifi {US 9514753 B2) – see paragraph 10, on pg 9 of the Office Action,

Claims 18 and 21-22 were rejected under 35 U.S.C. 103 as being unpatentable over Lawrence (US 2014/0108800 Al), Cheng (US 2017/109514 Al), Aura (US 2006/0020796 Al) and Sakamoto (US 2008/0181403 Al) in view of in view of Chul-min(US 20040221153 Al) – see paragraph 12, on pg 10 of the Office Action,

Claim 24 was rejected under 35 U.S.C. 103 as being unpatentable over Lawrence (US 2014/0108800 Al) and Aura (US 2006/0020796 Al)in view of Sakamoto (US 2008/0181403 Al) – see paragraph 18, on pg 13 of the Office Action,

Claims 23 was rejected under 35 U.S.C. 103 as being unpatentable over Lawrence (US 2014/0108800 Al) and Cheng (US 2017/109514 Al) – see paragraph 20, on pg 15 of the Office Action,

CLAIM AMENDMENTS

No claims have been amended. A response to the claim rejections is in order.

Claim Rejections - 35 U.S.C. §103

Claims 1-11 are rejected under U.S.C. §103 for alleged unpatentability over U.S. Patent Publication No. 2014/0108800 to Lawrence et al. ("Lawrence"), U.S. Patent Publication No. 2017/109514 to Cheng et al. ("Cheng"), U.S. Patent Publication No. 2006/0020796 to Aura et al. ("Aura"), in view of U.S. Patent Publication No. 2008/0181403 to Sakamoto et al. ("Sakamoto"). Applicant respectfully traverses this rejection.

At the outset, the mere fact of need to combine 4 documents in order to arrive at the subject-matter of claim 15 should be considered as an indicia of non-obviousness.

On a second note, the Applicant wishes to stress out that the idea underlying the invention is to avoid the bandwidth-related problems found in the prior art that, once the user captures the context data as defined by the authentication policy, he/she needs to send that entire and private information to the authentication server for its subsequent authentication.

This comes because the authentication policies requiring environment or context input are, unlike usernames and passwords, not fixed and may slightly differ in an acceptable manner. Therefore, if the protocol requires simply hashing the data packet before being sent, to save bandwidth while avoiding disclosing private data, the data originally captured should be identical to the template stored in the server, which is statistically impossible.

Thus, first, the present invention dispense with uploading the entire captured signal of the environment that needs several Mb while, second, still allows the server to authenticate the received data even if slightly differs in an acceptable manner with the stored template.

As it will be discussed herein-below, none of the cited documents addresses this very same problem or proposes a solution which could be applicable to solve it.

1. US 2014/0108800 A1 - Lawrence

Briefly, **Lawrence** addresses multi-factor authentication methods and, notably, discloses that when geolocation information is required for user's authentication it shall be transmitted by the client device to the authentication server which usually takes a long time. In [0034] it is stated an example of time delay between sending the information by the user device until arriving at the server side.

In [0032], it is set out that this significant amount of time may be leveraged by a spoofer to generate a false geothentication signal, for example, by creating a false data set that would mislead a time and/or location of the client device to the authentication server.

To solve this time delay-related issue, Lawrence proposes ([004]-[005]) sending by the client device hash value of the data block that enables authentication to the server, and also the data block itself.

Therefore, the server first receives the hash value and stores the time when this hash value is actually received at server side. Then, the server receives the actual data block comprising the alleged transmission signal data. At server's side, a hash value of the received data block is computed, and its receiving time calculated based on the alleged transmission signal data.

A timely possession of the received data block by the client device is authenticated based on a comparison of the computed hash value to the received hash value and a comparison of the hash value receiving time to the estimated transmission signal receiving time by the client.

Thus, Lawrence simply teaches sending in advance a hash of the data pack to have a reliable time stamping which is afterward compared with the actual data packet received. That is, there is the need of sending anyway the data packet to the server, which is exactly what our invention attempts to avoid for the bandwidth issues commented.

Consequently, as confirmed by the examiner, Lawrence does not disclose or suggest the following features:

- collecting, based on a predetermined authentication policy, at least one context data element;

- generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and

- authenticating successfully or not based on the generated hash distance, as an authentication step.

2. US 2017/109514 A1 - Cheng

Cheng aims at easing the tedious ways utilized to access the mobile devices which sometimes may delay important and time-sensitive access to the mobile device (e.g., in time-critical conditions). See [003] of Cheng.

According to its general description, for instance as per figure 1, there is a computing system with sensors able to capture activity context inputs and biometric inputs. In particular, a user authentication subsystem embodied in this computing system analyzes and interprets these inputs, and identifies therefrom the activity context and biometric signature expressed by one or more of the participants over time and in a substantially continuous fashion.

Then, the user authentication subsystem assesses the level of access control via access control module based on the score generated by authentication module. Using the activity context, the user authentication subsystem selects a biometric signature of the specific user, which is passed to the authentication module to either generate a score (if there is a match with a pre-stored one) or generate a new biometric key which will be stored in the enrolled user model. See [019]-[020] of Cheng.

First, Applicant wishes to remark that the whole authentication process takes place within the very same computing system, so in the proposed authentication method of Cheng there is no need to send any information or data packet outside. And, especially, Cheng does not focus on bandwidth restrictions or saving as the present invention does.

Hence, there is no incentive for the skilled person to consult this document.

Second, as everything happens internally to the computing system, there is no need to compute hashes and, especially, calculating hash distances for subsequent authentication.

Thus, to sum up, Cheng does not disclose or suggest the following features:

> *- collecting, based on a predetermined authentication policy, at least one context data element;*
>
> *- generating, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;*
>
> *- sending the generated hash;*
>
> *- generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and*
>
> *- authenticating successfully or not based on the generated hash distance, as an authentication step.*

3. US 2006/0020796 A1 - Aura

Aura addresses the associated problems about handling and memorizing long security codes when humans are used as secure channels. For instance, it is described that human users have a limited capability to remember long security codes, and if the security code is long enough, a human user may have difficulty entering the security code correctly. Security codes need to have long values (e.g., 50-80 bits) in order to be secure against brute-force attacks.

Thus, it proposes using a specific mechanism: extended Cryptographically Generated Addresses (ECGA). To generate an ECGA, an address owner computes two hash values using a public key and other parameters. A second hash value sets an input parameter for a first hash value, and at least a portion of the network address is derived from the first hash value. The combination of the two hash values increases the computational complexity of generating new addresses and, consequently, the cost of brute-force attacks.

Deep diving on the cited paragraphs by the examiner, namely on [0074], the examiner considers that this excerpt anticipates generating a *hash distance*. Applicant disagrees for the ensuing reasons.

The claimed feature under discussion is reproduced herein:

> *- generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and*

And [074] of Aura is also reproduced:

> A future cost of brute force attacks may be implied by the cost of generating the ECGA, e.g., the computing power of the computing system generating the ECGA. For example, the input N*Sec (e.g., Sec 302 of FIG. 3) may be replaced by a time input parameter indicating a time to be used for the address generation. In this manner, the generation of the second hash value may be based on the speed of the computing device generating the second hash value. The time input parameter may be set or initialized (such as in step 1102) by any suitable party, such as a device manufacturer or operating system vendor or by the user and may be set to the time that the user may be willing to spend on ECGA generation. For example, the time input may be set within a range of approximately 1-60 seconds if the user is waiting for the computations to approximately 1 CPU day or more if the computation is done slowly in the background. If the ECGA generation is done by a fast computer or dedicated machine other than the device for which the address in intended, the computation time may be set depending on the capacity of the machine used for the ECGA generation. More particularly, rather than having an input N*Sec 302 based on a number referring to a number of bits, the time parameter which is input to the ECGA generator 312 may refer to the time to compute the second hash value 500 of FIG. 5. The time parameter may be in any suitable form and/or units, such as an integer or real number value in seconds, CPU cycles, and the like. The ECGA generator may compute multiple second hash values during a time period defined by the time parameter input, and the output second hash value 500 may be selected as the **'most secure'** hash value generated in that time. The most secure hash value may be determined in any suitable manner, such as by the generated hash value in the input time which has the **greatest number of zero bits**. If the number of zero bits is expressed as N*Sec, where Sec is a security parameter encoded in some bits of the address, the most secure hash value may be determined by selecting the hash value that has the greatest number of zero bits rounded down to the nearest integer multiple of N. The greatest number of zero bits may be in a predetermined portion of the hash value (such as a predetermined number of the left-most bits), may be the greatest number of zero bits within the complete computed hash value, may be the greatest number of sequential zero bits within the computed hash value, the greatest hash extension, and the like.

Briefly, it explains that the security input parameter (N*Sec) can be replaced by a time input parameter indicating a time to be used for the address generation. For example, the time input may be set within a range of approximately 1-60 seconds if the user is waiting for the computations to approximately 1 CPU day or more if the computation is done slowly in the background.

That is, in this approach, the ECGA generator computes multiple second hash values during a time period defined by the time parameter input, and the output second hash value is selected as the 'most secure' hash value generated in that time based on a specific criteria. This criterion is e.g., the hash value within the input time having the greatest number of zero bits.

Nevertheless, the present invention does not want to set a specific time window and generate in advance the hashes. Instead, the present invention wants to authenticate the current and genuine context of the user according to his authentication policy. This means that the assessment disclosed in Aura is not directed to authentication purposes but simply to select in advance the most secure hash value.

As a matter of fact, Aura's content teaches away the present invention because suggests setting a time window for calculating in advance the hashes and store them in the meantime for their subsequent local assessment before being sent outside.

Thus, in Applicant's opinion, Aura does not disclose or suggest the following features:

- collecting, based on a predetermined authentication policy, at least one context data element;

- constituting (28), based on the at least one collected context data element, a data packet;

- generating (220), as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and

- authenticating (224) successfully or not (223) based on the generated hash distance, as an authentication step.

4. US 2008/0181403 A1 - Sakamoto

Finally, Sakamoto describes an authenticating system ([0021]) based on:

- a client apparatus that includes:
    - an authenticating information inputter for inputting ID and password of the user;
    - a client-side hash value creator for creating
        - a first hash value from the authentication information by employing a first hash algorithm that corresponds to a first hash algorithm identifier transmitted from the server apparatus, and
        - a second hash value from the first hash value and a random number transmitted from the server apparatus by employing the first hash algorithm; and
    - an authentication request manager for transmitting messages with a server
- the server apparatus that includes:

- a user information storage including
  - a second hash algorithm identifier that respectively corresponds for each the identification information of the user, and
  - a third hash value pre-created from the authentication information including the identification information and the password of the user by employing a second hash algorithm that corresponds to this hash algorithm identifier;
- a random number creator for creating a random number;
- a server-side hash value creator for creating a hash value; and
- an authentication information manager for, transmitting messages with the client apparatus.

Thus, it describes a authentication system formed by a client-side apparatus and a server communicating to each other. That is, the server instructs the client apparatus about which algorithm should use to compute the hash and further provides a random number to validate the received information afterwards.

This has nothing to do with the solution sets forth in the application or even the problem it attempts to solve.

Accordingly, Sakamoto does not disclose or suggest the following features:

- collecting, based on a predetermined authentication policy, at least one context data element;

- constituting, based on the at least one collected context data element, a data packet;

- sending the generated hash;

- generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and

- authenticating successfully or not based on the generated hash distance, as an authentication step.

That is, if there is no calculation of the hash distance, there cannot be an authentication based on this result.

Consequently, none of the cited documents either recites or suggests *inter alia* the steps of:

i. generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash, and
ii. authenticating successfully or not based on the generated hash distance, as an authentication step.

CONCLUSION

Accordingly, for at least the reasons set forth above, the combination of documents cannot support a prima facie case for rejecting claim 16 under 35 U.S.C. §103(a). As such, Applicant respectfully submits that independent claim 16 is patentably distinct from Lawrence, Cheng, Aura, in view of Sakamoto and hence requests that the rejection be withdrawn.

Independent claims 23, 24 and 25 although different in scope, recites at least some of the same distinguishing features as recited in claim 16. Accordingly, the same arguments apply *mutatis mutandis* to independent claim 23, 24 and 25.

By virtue of the dependency of claims 17-22 on independent claim 16 these dependent claims are also novel and non-obvious over the cited documents.

The Applicant believes that this application is now in full condition for allowance. Allowance of the application, accordingly, is respectfully requested. The Applicant respectfully requests that the Examiner please call the undersigned if clarification is needed on any matter within this Response, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

Date: February 15, 2022

/Marc Boillot/
Marc A. Boillot
USPTO Reg. No.: 56,164
Telephone: (954) 658-0418

Customer No.: 180929

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/958,252	06/26/2020	Fabrice DELHOSTE	1032326-001016

CONFIRMATION NO. 5318

180929
THALES DIS CPL US
THALES DIS USA Inc.
4690 Millennium Drive
Belcamp, MD 21017

POA ACCEPTANCE LETTER

OC000000129097698

Date Mailed: 10/15/2021

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/08/2021.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/atesfai/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/958,252	06/26/2020	Fabrice DELHOSTE	1032326-001016

CONFIRMATION NO. 5318

21839
BUCHANAN, INGERSOLL & ROONEY PC
1737 KING STREET
SUITE 500
ALEXANDRIA, VA 22314-2727

POWER OF ATTORNEY NOTICE

OC000000129097685

Date Mailed: 10/15/2021

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/08/2021.

- The Power of Attorney to you in this application has been revoked by the applicant. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/atesfai/

PTO/AIA/80 (07-17)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no person is required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

[X] Practitioners associated with Customer Number: 180929

OR

[X] Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number
Marc BOILLOT	56164		

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

[X] The address associated with Customer Number: 180929

OR

[ ]

Firm or individual name		
Address		
City	State	Zip
Country		
Telephone	Email	

Assignee name and address: THALES DIS FRANCE SA - 6, rue de la Verrerie - 92190 MEUDON-FRANCE

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of the practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee.

Signature	Date Nov. 23, 2021
Name Patrick Mouchart	Telephone +33 4.42.36.34.51
Title Chief Executive Officer	

This collection of information is required by 37 CFR 1.31, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public, which is to update (and by the USPTO to process) the file of a patent or reexamination proceeding. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 18 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt	
EFS ID:	43989093
Application Number:	16958252
International Application Number:	
Confirmation Number:	5318
Title of Invention:	AUTHENTICATION METHOD, DEVICE AND SYSTEM
First Named Inventor/Applicant Name:	Fabrice DELHOSTE
Customer Number:	21839
Filer:	James A. LaBarre/Nina Leta
Filer Authorized By:	James A. LaBarre
Attorney Docket Number:	1032326-001016
Receipt Date:	08-OCT-2021
Filing Date:	26-JUN-2020
Time Stamp:	16:51:01
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assignee showing of ownership per 37 CFR 3.73	Statement_Under_37_CFR_3_73.pdf	3850916 53e3b5f5c2a4292d5e6d7f1ffb75a592fa7dba65	no	3
Warnings:					

Information:					
2	Power of Attorney	THALES_DIS_FRANCE_SA_POA.pdf	234707 f076ed0da8f7e2548c00679c1c22400e0b9a593c	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	4085623	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: THALES DIS FRANCE SA

Application No./Patent No.: 16/958,252 Filed/Issue Date: 2020-06-26

Titled: AUTHENTICATION METHOD, DEVICE AND SYSTEM

THALES DIS FRANCE SA, a Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Fabrice Delhoste, Frederic Paillart, Sebastien | To: THALES DIS FRANCE SA

   The document was recorded in the United States Patent and Trademark Office at

   Reel 054960, Frame 0332, or for which a copy thereof is attached.

2. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at

   Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/James A LaBarre/	2021-10-08
Signature	Date
James A. LaBarre	28,632
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/958,252	06/26/2020	Fabrice DELHOSTE	1032326-001016	5318

21839 7590 09/16/2021

BUCHANAN, INGERSOLL & ROONEY PC
1737 KING STREET
SUITE 500
ALEXANDRIA, VA 22314-2727

EXAMINER	
SHAAWAT, MAYASA A.	

ART UNIT	PAPER NUMBER
2433	

NOTIFICATION DATE	DELIVERY MODE
09/16/2021	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPDOC1@BIPC.com

Office Action Summary	Application No. 16/958,252	Applicant(s) DELHOSTE et al.	
	Examiner MAYASA A SHAAWAT	Art Unit 2433	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 06/26/2020.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 16-25 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 16-25 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 06/26/2020 is/are: a)☐ accepted or b)☑ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☑ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☑ All b)☐ Some** c)☐ None of the:

1.☑ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

2. This is the initial office action that has been issued in response to patent application 16/958,252, filed on 06/26/2020. Claims 1-15 are cancelled. Claims 16-25 as originally filed and are currently pending and have been considered below.

Specification

3. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Drawings

4. The drawings are objected to under 37 CFR 1.83(a) because **they fail to show details of the drawings** as described in the specification. Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any

amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 16, 20 and 25 are rejected under 35 U.S.C. 103 as being unpatentable over Lawrence (US 2014/0108800 A1), Cheng (US 2017/109514 A1) and Aura (US 2006/0020796 A1) in view of Sakamoto (US 2008/0181403 A1).

7. **Regarding Claim 16**, Lawrence and Cheng disclose, an authentication method comprising:

Lawrence does not explicitly disclose the following limitations that Cheng teaches:

- collecting, based on a predetermined authentication policy, at least one context data element (**Cheng, [0031]**, ***the utilization of a user's activity context for continuous authentication, embodiment of the present invention may also be used for providing alerts. An alert generated in response to the detection of a predetermined activity context***);

It would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to include an authentication policy that is collected at the data element wherein at least one context is existing.

- constituting a data packet, based on the at least one collected context data element (**Lawrence, [0053]**, ***the client device 108 seeded by the digital samples 226 collected by the client device in the data block 138 and authenticate***); -

generating a hash, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm (Lawrence, [0070], *The function 242, may comprise for example but without limitation, a Secure Hash Algorithm or other algorithm capable of generating a repeatable hash value such as the hash value 152 for the same data block such as the data block 138*); - sending the generated hash (Lawrence, [0058], *sends hash value*);

Lawrence and Cheng does not explicitly disclose the following limitations that Aura teaches:

- generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash (Aura, [0074], *in a predetermined portion of the hash value (such as a predetermined number of the left-most bits), may be the greatest number of zero bits within the complete computed hash value, may be the greatest number of sequential zero bits within the computed hash value*);

Lawrence, Cheng and Aura does not explicitly disclose the following limitations that Sakamoto teaches:

It would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to include the generated hash between the determined hash.

Lawrence, Cheng and Aura does not explicitly disclose the following limitations that Sakamoto teaches:

and - authenticating successfully or not based on the generated hash distance, as an authentication step (**Sakamoto, [0002], *an authenticating system, an authenticating method, and an authenticating program that can be successively utilized also in a case where a hash algorithm***)

8. **Regarding Claim 20**, Lawrence, Cheng, Aura and Sakamoto disclose, the method according to claim 16,
Lawrence does not explicitly disclose the following limitations that Cheng teaches:
wherein, prior to constituting the data packet, the method further comprises grouping together, according to the authentication policy, at least two context data elements comprised within the at least one context data element, to constitute at least one corresponding context data group (**Cheng, [0050], *modules and/or data structures may be combined or divided into sub-modules, sub-processes or other units of computer code or data as may be required by a particular design or implementation of the user authentication subsystem 110.***).

It would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed

invention combine two of the context data from the information provided in the authentication policy and include at least one corresponding context data.

9. **Regarding Claim 25**, Lawrence, Cheng, Aura, Sakamoto disclose, an authentication system, comprising a first authentication device and at least one second authentication device, wherein the first authentication device is configured to:

Lawrence does not explicitly disclose the following limitations that Cheng teaches:

- collect at least one context data element, based on a predetermined authentication policy (**Cheng**, [0031], *the utilization of a user's activity context for continuous authentication, embodiment of the present invention may also be used for providing alerts. an alert generated in response to the detection of a predetermined activity context [0024], the data signals produced by the sensing device(s) 126 provide the activity context inputs 128 and/or the biometric inputs 130 that are analyzed by the user authentication subsystem 110.);* - constitute a data packet, based on the at least one collected context data element (**Lawrence**, [0053], *the client device 108 seeded by the digital samples 226 collected by the client device in the data block 138 and authenticate*); - generate

a hash, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm (Lawrence, [0070], *The function 242, may comprise for example but without limitation, a Secure Hash Algorithm or other algorithm capable of generating a repeatable hash value such as the hash value 152 for the same data block such as the data block 138.*); and - send to the second authentication device, the generated hash (Lawrence, [0058], *sends hash value*); - and wherein the second authentication device is configured to: - receive the generated hash from the first device (Lawrence, [0006], *a client device receives a received hash value*);

Lawrence and Cheng does not explicitly disclose the following limitations that Aura teaches:

- generate a hash distance between the generated hash and a predetermined reference hash (Aura, [0074], *in a predetermined portion of the hash value (such as a predetermined number of the left-most bits), may be the greatest number of zero bits within the complete computed hash value, may be the greatest number of sequential zero bits within the computed hash value*);

and - authenticate successfully or not based on the generated hash distance (Sakamoto, [0002], *an authenticating system, an authenticating method, and an authenticating program that can be successively utilized also in a case where a hash algorithm.*).

10. Claims 17 is rejected under 35 U.S.C. 103 as being unpatentable over Lawrence (US 2014/0108800 A1), Cheng (US 2017/109514 A1), Aura (US 2006/0020796 A1) and Sakamoto (US 2008/0181403 A1) in view of Sharifi (US 9514753 B2).

11. Regarding Claim 17, Lawrence, Cheng, Aura, Sakamot and Sharifi disclose, the method according to claim 16, wherein, the predetermined hash type algorithm comprises a locality sensitive hash type algorithm, and wherein the method further comprises, as the hash distance generation step and the authentication step, the following steps:

Lawrence, Cheng Aura, Sakamoto does not disclose the following limitations that Sharifi teaches:

- generating a score, by using the locality sensitive hash type algorithm, as a level of similarity between the generated hash and the predetermined reference hash (**Sharifi, Col. 19, lines 25-28,** *Comparing the speaker vectors in the set with the utterance vector includes determining similarity scores that each indicate a degree of similarity. Col. 9, lines 60-61, For each speaker vector 130 a-130 c, a hash value may be determined for each of multiple hash functions 140*);

Lawrence and Cheng does not disclose the following limitations that Sharifi teaches:

- comparing the score to a predetermined threshold value (**Sharifi, Col. 12, lines 54-55,** ***similarity score that satisfies the threshold***);

It would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to include a score that is generated using levels of similarities for predetermined reference hash and comparing the score to the threshold.

- authenticating successfully only if the score is equal to or greater than the predetermined threshold value (**Lawrence, [0050],** ***the data block 138 has effectively been validated, the data block 138 can reliably be processed to authenticate the time t_2 and/or the location 122 of the client device 108. [0086], he computed hash value 322 match, and if the time difference 322 (t_1-t_{2est}) is below a time threshold value, the authentication processor 300 authenticates possession).***

12. Claims 18 and 21-22 are rejected under 35 U.S.C. 103 as being unpatentable over Lawrence (US 2014/0108800 A1), Cheng (US 2017/109514 A1), Aura (US 2006/0020796 A1) and Sakamoto (US 2008/0181403 A1) in view of in view of Chul-min(US 20040221153 A1)

13. **Regarding Claim 18**, Lawrence, Cheng, Aura, Sakamoto and Chul-min disclose, the method according to claim 16,

Lawrence, Cheng, Aura, Sakamoto does not explicitly disclose the following limitations that Chil-min teaches:

wherein, prior to generating the hash, the method further comprises sorting, according to a numerical order, the at least one collected context data element within the data packet (**Chul-min, Abstract, *data packets as a combination value, which is obtained by dividing the fixed width by the variable width, and combining the same number of sequentially received variable***).

It would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to include the generated hash and sorting the method in numerical order for one collected context data.

14. **Regarding Claim 21**, Lawrence, Cheng, Aura, Sakamoto and Chul-min disclose, the method according to claim 16,

Lawrence, Cheng, Aura, Sakamoto does not explicitly disclose the following limitations that Chil-min teaches:

wherein, prior to generating the hash, the method further comprises ciphering the data packet, according to the authentication policy (**Chul-min, [0050], *generates a hash code providing authentication for an entire fixed width data packet. [0041], he enciphering unit 22 enciphers a fixed width data***

packet. [0051], AH engine generates an authentication code of an entire data packet).

It would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to cipher the data packet with the information given from the authentication policy.

15. **Regarding Claim 22**, Lawrence, Cheng, Aura, Sakamoto and Chul-min disclose, the method according to claim 21, **Lawrence, Cheng, Aura, Sakamoto does not explicitly disclose the following limitations that Chil-min teaches:**
wherein a key used for the data packet ciphering includes a key generated by using a hash-based message authentication code key type derivation function (**Chul-min, [0050], *the AH engine using a hash message authentication code (HMAC)-message digest function 95 (MD5) algorithm, 32-bit data is input and enciphered and 32-bit cipher data is output. HMAC-MD5 is a secret key algorithm providing authentication***).

It would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to include the key used to cipher the data packet generating the HMAC authentication code.

16. Claims 19 is are rejected under 35 U.S.C. 103 as being unpatentable over Lawrence (US 2014/0108800 A1), Cheng (US 2017/109514 A1), Aura (US 2006/0020796 A1) and Sakamoto (US 2008/0181403 A1) in view of Bisikalo (EP 2924603 A2).

17. **Regarding Claim 19**, Lawrence, Cheng, Aura, Sakamoto and Bisikalo disclose, the method according to claim 16, **Lawrence, Cheng, Aura, Sakamoto does not explicitly disclose the following limitations that Bisikalo teaches:**
wherein, prior to generating the hash, the method further comprises weighting, according to the authentication policy, the at least one context data element (**Bisikalo, [0031], *financial institution may want to weigh the audio element 406 more heavily in the total score than a visual element (e.g., 408) because the institution can utilize speech recognition technology to identify the user with great precision).***

It would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to include weighing the hash for the context data element within the authentication policy

18. Claim 24 is rejected under 35 U.S.C. 103 as being unpatentable over Lawrence (US 2014/0108800 A1) and Aura (US 2006/0020796 A1)in view of Sakamoto (US 2008/0181403 A1)

19. Regarding Claim 24, Lawrence and Aura disclose, a second authentication device, wherein the second authentication device is configured to: - receive a generated hash (Lawrence, [0006], *a client device receives a received hash value*);

Lawrence does not explicitly disclose the following limitations that Aura teaches:

- generate a hash distance between the generated hash and a predetermined reference hash (Aura, [0074], *in a predetermined portion of the hash value (such as a predetermined number of the left-most bits), may be the greatest number of zero bits within the complete computed hash value, may be the greatest number of sequential zero bits within the computed hash value*);

It would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to include the generated hash between the determined hash.

Lawrence and Aura does not explicitly disclose the following limitations that Sakamoto teaches:

and - authenticate successfully or not based on the generated hash distance (Sakamoto, [0002], *an authenticating system, an authenticating method, and an authenticating program that can be successively utilized also in a case where a hash algorithm.*).

20. Claims 23 is rejected under 35 U.S.C. 103 as being unpatentable over Lawrence (US 2014/0108800 A1) and Cheng (US 2017/109514 A1).

21. Regarding Claim 23, Lawrence and Cheng disclose, a first authentication device, wherein the first authentication device is configured to:

Lawrence does not explicitly disclose the following limitations that Cheng teaches:

- collect at least one context data element, based on a predetermined authentication policy (Cheng, [0031], *the utilization of a user's activity context for continuous authentication, embodiment of the present invention may also be used for providing alerts. an alert generated in response to the detection of a predetermined activity context [0024], the data signals produced by the sensing device(s) 126 provide the activity context inputs 128 and/or the biometric inputs 130 that are analyzed by the user authentication subsystem 110.*); - constitute a data packet, based on the at least one collected context data element (Lawrence, [0053], *the client device 108 seeded by the digital samples 226 collected by the client device in the data block 138 and authenticate*); - generate

a hash, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm (**Lawrence, [0070], *The function 242, may comprise for example but without limitation, a Secure Hash Algorithm or other algorithm capable of generating a repeatable hash value such as the hash value 152 for the same data block such as the data block 138.***); and - send the generated hash to a second authentication device (**Lawrence, [0058], *sends hash value***).

Conclusion

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to **MAYASA SHAAWAT** whose telephone number is (571)272-3939. The examiner can normally be reached on M-F, 8 AM TO 5 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **JEFFREY PWU** can be reached on (571)272-6789. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

Information regarding the status of an application may be

obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see https://ppair-my.uspto.gov/pair/PrivatePair. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MAYASA SHAAWAT/
Examiner, Art Unit 2433

/JEFFREY C PWU/
Supervisory Patent Examiner, Art Unit 2433

Notice of References Cited	Application/Control No. 16/958,252	Applicant(s)/Patent Under Reexamination DELHOSTE et al.	
	Examiner MAYASA A SHAAWAT	Art Unit 2433	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20140108800-A1	04-2014	Lawrence; David	H04L9/3297	713/168
*	B	US-20170109514-A1	04-2017	Cheng; Hui	G06F21/316	1/1
*	C	US-20060020796-A1	01-2006	Aura; Tuomas	H04L63/123	713/168
*	D	US-9514753-B2	12-2016	Sharifi; Matthew	G10L25/51	1/1
*	E	US-20080181403-A1	07-2008	SAKAMOTO; YU	H04L9/3236	380/258
*	F	US-20040221153-A1	11-2004	Kim, Chul-min	H04L9/0637	713/150
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N	EP-2924603-A2	09-2015	EP	BISIKALO DMITRY	G06F21/32
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/958,252	DELHOSTE et al.
	Examiner	**Art Unit**
	MAYASA A SHAAWAT	2433

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/07/2021								
	1	-								
	2	-								
	3	-								
	4	-								
	5	-								
	6	-								
	7	-								
	8	-								
	9	-								
	10	-								
	11	-								
	12	-								
	13	-								
	14	-								
	15	-								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								

Thales Exhibit 2001, Page 107 of 339
Okta v. Thales DIS France - IPR2026-00278

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/958,252	DELHOSTE et al.
	Examiner	Art Unit
	MAYASA A SHAAWAT	2433

CPC - Searched*		
Symbol	Date	Examiner
H04L9/0643, H04L9/0866 , H04L9/3231, H04L9/3242	09/08/2021	MAS

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

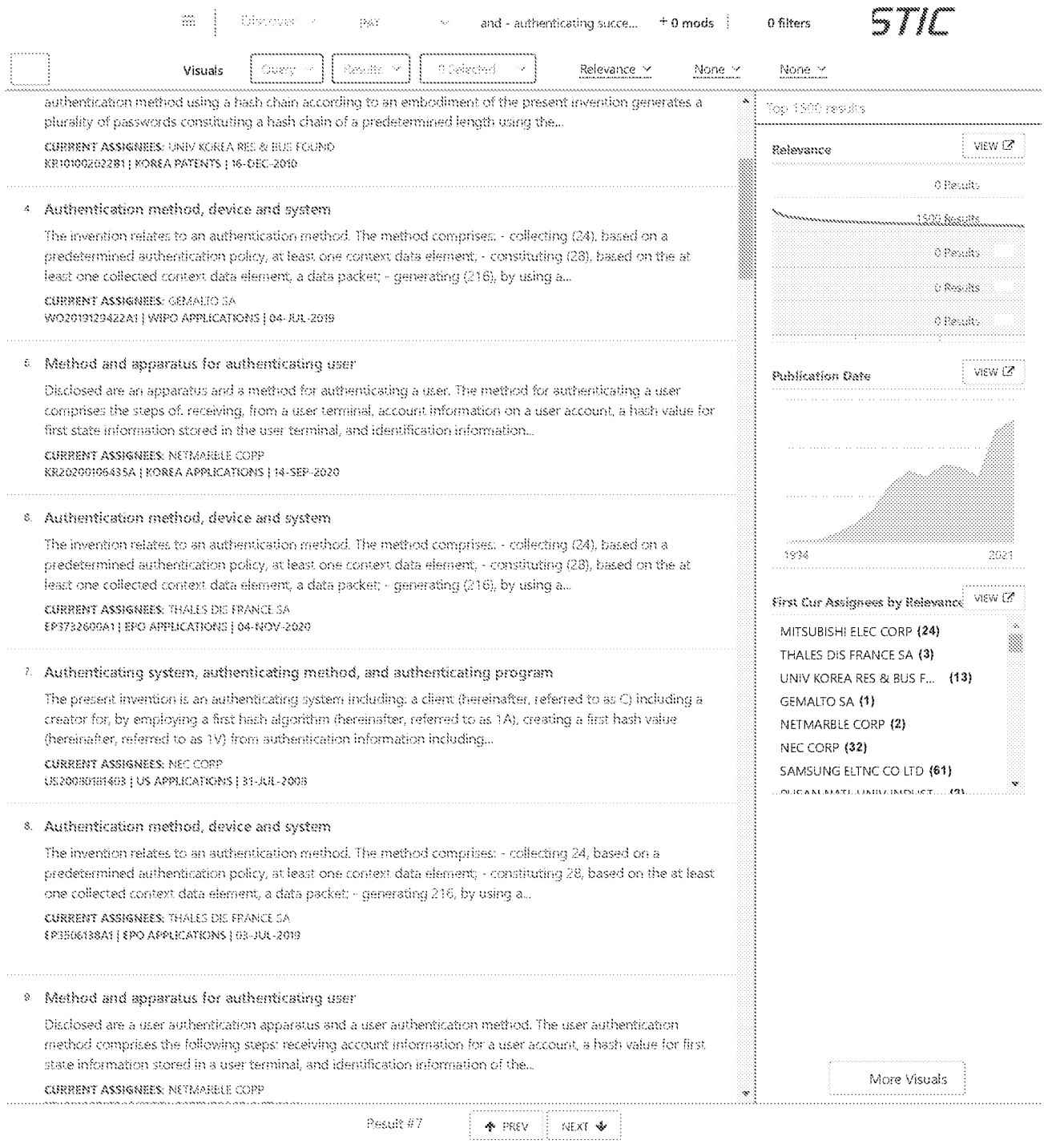
* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
H04L9/0643, H04L9/0866 , H04L9/3231, H04L9/3242	09/08/2021	MAS
PE2E search	09/07/2021	MAS
inventor and applicant search	09/07/2021	MAS
ip.com search	09/07/2021	MAS
espacenet.com	09/07/2021	MAS

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/MAYASA A. SHAAWAT/ Examiner, Art Unit 2433	

Thales Exhibit 2001, Page 108 of 339
Okta v. Thales DIS France - IPR2026-00278



Thales Exhibit 2001, Page 109 of 339
Okta v. Thales DIS France - IPR2026-00278

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	76	((("THALES") near3 ("DIS") near3 ("FRANCE") near3 ("SA"))).AS,AANM.	(USPAT)	OR	ON	ON	2021/09/07 12:14 PM
L2	5	((("DELHOSTE") near3 ("Fabrice")) OR (("PAILLART") near3 ("Frdric")) OR (("PETIT") near3 ("Sbastien"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/07 12:14 PM
L3	165	(L1 L2) AND authentication	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/07 12:24 PM
L4	2	((authentication ADJ policy) SAME data SAME element SAME hash WITH algorithm)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/07 12:27 PM
L5	0	((authentication OR validat$ OR authorize) SAME (data ADJ packet) SAME (collected OR collection) WITH context SAME hash SAME algorith)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 09:17 AM
L6	2	((authentication OR validat$ OR authorize) SAME (data ADJ packet) SAME (collected OR collection) WITH context SAME hash)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 09:17 AM
L7	0	((authentication OR validat$ OR authorize) SAME (data ADJ packet) SAME (collected OR collection) WITH context SAME (hash ADJ algorithm))	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 09:21 AM
L8	7	((authentication OR validat$ OR authorize) SAME (data ADJ packet) SAME (collected OR collection) WITH context)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 09:28 AM
L9	2	((authentication OR validat$ OR authorize) SAME (data ADJ	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 09:29 AM

		packet) SAME (collected OR collection) WITH context) AND (H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.					
L10	29635	(H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 09:31 AM
L11	403	(authentication SAME (data ADJ packet)) AND (H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 09:55 AM
L12	1	(weighting SAME (authentication ADJ policy) SAME context WITH (data ADJ element)) AND (H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 10:30 AM
L13	0	((data ADJ packet) WITH ciphering WITH (hash OR HMAC) SAME (authentication ADJ code) SAME derive) AND (H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 04:48 PM
L14	1	((data ADJ packet) WITH ciphering WITH (hash OR HMAC) SAME (authentication ADJ code)) AND (H04L9/0643 OR H04L9/0866 OR H04L9/3231 OR H04L9/3242).cpc.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 04:48 PM
L15	1	((data ADJ packet) WITH ciphering WITH (hash OR HMAC) SAME (authentication ADJ code))	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 04:48 PM
L16	6	((data ADJ packet) WITH cipher$ WITH (hash OR HMAC) SAME (authentication	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/08 04:49 PM

		ADJ code))					
L17	1	((data ADJ packet) WITH (hash OR HMAC) WITH distance SAME authentication WITH successfully)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/09 12:36 PM
L18	1	((data ADJ packet) WITH (hash OR HMAC) WITH (distance OR length OR range) SAME authentication WITH successfully)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2021/09/09 12:39 PM

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 924 603 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
30.09.2015 Bulletin 2015/40

(51) Int Cl.:
G06F 21/32 *(2013.01)* ***G06K 9/00*** *(2006.01)*
G10L 17/00 *(2013.01)*

(21) Application number: **15160817.1**

(22) Date of filing: **25.03.2015**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
MA

(30) Priority: **25.03.2014 US 201414224901**

(71) Applicant: **FMR LLC**
Boston, MA 02210 (US)

(72) Inventors:
- **McDonough, John**
  Boston, MA 02210 (US)
- **Hromi, Jonathan**
  Boston, MA 02210 (US)
- **Stern, Hadley Rupert**
  Boston, MA 02210 (US)
- **Bisikalo, Dmitry**
  Boston, MA 02210 (US)

(74) Representative: **Greene, Simon Kenneth**
Elkington and Fife LLP
Prospect House
8 Pembroke Road
Sevenoaks, Kent TN13 1XR (GB)

(54) METHOD AND SYSTEM FOR USER AUTHENTICATION BASED ON BIOMETRICS, CLOTHES WEARING AND SURROUNDING SCENE

(57) Methods and apparatuses, including computer program products, are described for authentication using a video signature. A computing device receives a request to access a secure resource, and the request includes a first video segment comprising a plurality of visual and audio elements, wherein at least a first one of the visual elements comprises a physical characteristic of the user, e.g. biometrics, at least a second one of the visual elements comprises a physical object in proximity to the user, e.g. an object worn / owned by the user, and at least a third one of the visual elements comprises an element of the environment surrounding the user, e.g. determining geolocation. The computing device analyzes one or more of the plurality of visual and audio elements in the first video segment to determine a value associated with each of the one or more analyzed elements. The computing device calculates a total score for the first video segment based upon the value associated with each of the one or more analyzed elements. The computing device compares the total score for the first video segment to a score associated with a second video segment associated with the computing device. The computing device determines whether access to the secure resource is permitted based upon the comparison step.

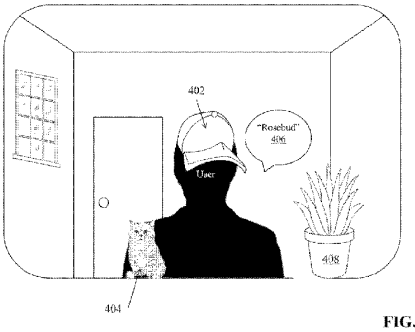


FIG. 4

EP 2 924 603 A2

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] This application relates generally to methods and apparatuses, including computer program products, for authentication using a video signature.

[0002] Typical authentication mechanisms, such as username / password combinations, are susceptible to theft, spoofing, phishing, and other forms of fraudulent activity by impostors seeking access to a user's secure accounts or resources (e.g., websites, documents, databases). More robust authentication techniques, like biometric scanning, have not yet become widely available and can depend significantly on both the type of technology available to a user and the type of technology used by an entity monitoring access to a secure resource.

[0003] Many computing devices, especially mobile devices, are equipped with cameras that can be used to record and transmit video segments (e.g., still images, video clips). Video segments typically incorporate a variety of visual and audio elements that can be used to uniquely identify the video segment in question from other video segments.

[0004] Therefore, what is needed are methods and systems to leverage the video capture capability of computing devices to generate a video signature used in authenticating a user and/or computing device to a secure resource. The techniques described herein provide the advantage of generating a video signature through analysis of a user-created and submitted video segment that includes a plurality of distinct visual and audio elements, where the plurality of elements are analyzed to calculate a total score for the video segment. A video segment, submitted by a user and assigned a score, can be used as a video signature to authenticate subsequent attempts to access the secure resource, e.g., by comparing the visual and audio elements in a later-submitted video segment against the video signature associated with a previously-submitted video segment.

[0005] The invention, in one aspect, features a method for authentication using a video signature. A computing device receives a request to access a secure resource, and the request includes a first video segment comprising a plurality of visual and audio elements. The computing device analyzes one or more of the plurality of visual and audio elements in the first video segment to determine a value associated with each of the one or more analyzed elements. The computing device calculates a total score for the first video segment based upon the value associated with each of the one or more analyzed elements. The computing device compares the total score for the first video segment to a score associated with a second video segment associated with the computing device. The computing device determines whether access to the secure resource is permitted based upon the comparison step.

[0006] The invention, in another aspect, features a system for authentication using a video signature. The system includes a computing device configured to receive a request to access a secure resource, and the request includes a first video segment comprising a plurality of visual and audio elements. The computing device is configured to analyze one or more of the plurality of visual and audio elements in the first video segment to determine a value associated with each of the one or more analyzed elements. The computing device is configured to calculate a total score for the first video segment based upon the value associated with each of the one or more analyzed elements. The computing device is configured to compare the total score for the first video segment to a score associated with a second video segment associated with the computing device. The computing device is configured to determine whether access to the secure resource is permitted based upon the comparison step.

[0007] The invention, in another aspect, features a computer program product, tangibly embodied in a non-transitory computer readable storage medium, for authentication using a video signature. The computer program product includes instructions operable to cause a computing device to receive a request to access a secure resource, and the request includes a first video segment comprising a plurality of visual and audio elements. The computer program product includes instructions operable to cause the computing device to analyze one or more of the plurality of visual and audio elements in the first video segment to determine a value associated with each of the one or more analyzed elements. The computer program product includes instructions operable to cause the computing device to calculate a total score for the first video segment based upon the value associated with each of the one or more analyzed elements. The computer program product includes instructions operable to cause the computing device to compare the total score for the first video segment to a score associated with a second video segment associated with the computing device. The computer program product includes instructions operable to cause the computing device to determine whether access to the secure resource is permitted based upon the comparison step.

[0008] In a yet further aspect, the invention relates to a method for authentication using a video signature, the method comprising: receiving, by a computing device from a remote device associated with a user, a request to access a secure resource, the request including a first video segment comprising a plurality of visual and audio elements, wherein at least a first one of the visual elements comprises a physical characteristic of the user, at least a second one of the visual elements comprises a physical object in proximity to the user, and at least a third one of the visual elements comprises an element of the environment surrounding the user; determining, by the computing device, a plurality of characteristics associated with each of the plurality of visual and audio elements; assigning, by the computing device, a value to each of the characteristics based upon predetermined value information stored by the computing device; calculating, by the computing device, a total score for the first video segment based upon the value associated with each of the character-

Thales Exhibit 2001, Page 114 of 339
Okta v. Thales DIS France - IPR2026-00278

istics; comparing, by the computing device, the total score for the first video segment to a score associated with a second video segment previously received from the remote device; determining, by the computing device, whether to permit the remote device to access the secure resource based upon the comparison step; and connecting, by the computing device, the remote device to the secure resource if access is permitted.

[0009] Any of the above aspects can include one or more of the following features. In some embodiments, the analyzing step includes determining one or more characteristics associated with each of the one or more plurality of visual and audio elements, assigning a value to the characteristics based upon predetermined value information stored by the computing device, and storing the values for the characteristics. In some embodiments, the one or more characteristics include a position of a visual element, movement of a visual element, a color of a visual element, a type of a visual element, and an absence of a visual element. In some embodiments, the computing device performs a speech-to-text conversion on an audio element. In some embodiments, values are assigned to the characteristics based upon frequency of appearance within frames of the first video segment. In some embodiments, the predetermined value information is adjusted based upon preferences provided by a user of the computing device.

[0010] In some embodiments, the calculating step includes assigning a weight to one or more of the analyzed elements based upon a security profile at the computing device. In some embodiments, the comparing step further includes comparing the value associated with one of the analyzed elements in the first video segment to a value associated with an analyzed element in the second video segment, and determining a deviation value based upon the comparison of the analyzed element values. In some embodiments, the computing device aggregates the deviation value for the comparisons of each of the analyzed element values and determines whether the aggregated deviation value falls below a predetermined threshold.

[0011] In some embodiments, the plurality of visual and audio elements includes a visual representation of a user of the computing device. In some embodiments, the plurality of visual and audio elements includes an object in proximity to the user of the computing device. In some embodiments, the plurality of visual and audio elements includes a phrase spoken by the user of the computing device.

[0012] In some embodiments, the first video segment is captured using a camera connected to the computing device. In some embodiments, the computing device is a mobile device. In some embodiments, the secure resource is a website.

[0013] Other aspects and advantages of the invention will become apparent from the following detailed description, taken in conjunction with the accompanying drawings, illustrating the principles of the invention by way of example only.

[0014] The advantages of the invention described above, together with further advantages, may be better understood by referring to the following description taken in conjunction with the accompanying drawings. The drawings are not necessarily to scale, emphasis instead generally being placed upon illustrating the principles of the invention.

FIG. 1 is a block diagram of a system for authentication using a video signature, according to an embodiment of the invention.

FIG. 2 is a block diagram of a system for authentication using a video signature, according to an embodiment of the invention.

FIG. 3 is a flow diagram of a method for authentication using a video signature, according to an embodiment of the invention.

FIG. 4 is a diagram of an exemplary video segment to be analyzed to generate a video signature, according to an embodiment of the invention.

FIG. 5 is a diagram of an exemplary video segment to be authenticated using a video signature, according to an embodiment of the invention.

FIG. 6 is a diagram of another exemplary video segment to be authenticated using a video signature, according to an embodiment of the invention.

[0015] FIG. 1 is a block diagram of a system 100 for authentication using a video signature, according to an embodiment of the invention. The system 100 includes a client computing device 102, a camera device 103 coupled to client device 102, a communications network 104, a server computing device 106 that includes a video signature authentication module 108, and a database 110.

[0016] The client device 102 connects to the server computing device 106 via the communications network 104 in order to authenticate a video signature captured by the client device 102. Exemplary client devices include desktop computers, laptop computers, tablets, mobile devices, smartphones, and internet appliances. It should be appreciated that other types of computing devices that are capable of connecting to the server computing device 106 can be used without departing from the scope of invention. Although FIG. 1 depicts one client device 102, it should be appreciated that the system 100 can include any number of client devices.

[0017] A camera device 103 is coupled to client device 102. The camera device can be any type of digital video camera (e.g., webcam) that is capable of capturing and transmitting video images of the user and/or the client device 102. As will be described in greater detail below, the camera device is configured to capture images of the user and the area

Thales Exhibit 2001, Page 115 of 339
Okta v. Thales DIS France - IPR2026-00278

surrounding the user for purposes of performing authentication of the user and/or the client device. In some embodiments, the camera device 103 is embedded in the client device 102, for example, a smartphone with an integrated camera or a laptop computer with an integrated webcam. Although FIG. 1 depicts one camera device 103, it should be understood that the system 100 can include any number of camera devices.

[0018] The communication network 104 enables the client device 102 to communicate with the server computing device 106 in order to perform authentication procedures. The network 104 may be a local network, such as a LAN, or a wide area network, such as the Internet and/or a cellular network. In some embodiments, the network 104 is comprised of several discrete networks and/or sub-networks (e.g., cellular → Internet) that enable the client device 102 to communicate with the server computing device 106. It should be understood that the client device 102 can connect to the server computing device 106 via a wireless network (e.g., Bluetooth, WiFi, and so forth).

[0019] The server computing device 106 is a combination of hardware and software modules that authenticates a video signature captured by the client device 102 and enables access by the client device to a secure resource. The server computing device 106 includes a video signature authentication module 108. The module 108 is a hardware and/or software module that resides on the server computing device 106 to perform functions associated with authenticating the video signature provided by the client device 102. In some embodiments, the functionality of the module 108 is distributed among a plurality of computing devices. It should be appreciated that any number of computing devices, arranged in a variety of architectures, resources, and configurations (e.g., cluster computing, virtual computing, cloud computing) can be used without departing from the scope of the invention.

[0020] The system 100 also includes a database 110. The database 110 is coupled to the server computing device 106 and stores data used by the server computing device 106 to perform the video signature authentication functionality. The database 110 can be integrated with the server computing device 106 or be located on a separate computing device. An example database that can be used with the system 100 is MySQL™ available from Oracle Corp. of Redwood City, California.

[0021] FIG. 2 is a block diagram of a system 200 for authentication using a video signature, according to an embodiment of the invention. The system 200 of FIG. 2 is similar to the system 100 of FIG. 1; the system 200 includes client device 102, a camera device 103 coupled to client device 102, and a database 110. In FIG. 2, however, the client computing device 102 includes the video signature authentication module 108, enabling the client device to perform video signature authentication locally (i.e., without requiring traversal of the communications network 104 of FIG. 1). As shown in FIG. 2, the camera device 103 is embedded within the client device 102. It should be appreciated that other configurations of the client device 102 and camera device are contemplated within the scope of invention, such as a camera device 103 wirelessly connected to the client device 102.

[0022] FIG. 3 is a flow diagram of a method 300 for authentication using a video signature, using the system 100 of FIG. 1. It should be appreciated that the system 200 of FIG. 2 can also be used to perform the method 300 depicted in FIG. 3.

[0023] The server computing device 106 receives (302) a request to access a secure resource. In one example, a secure resource is a website or other service that is protected from public access and requires the submission and verification of authentication credentials by a user seeking access to the secure resource. The process of authenticating the user involves verifying the user's identity.

[0024] For example, a user of client device 102 can navigate to a financial institution's website in order to log in to his or her account. Typically, such websites require that the user provides a form of authentication credential (e.g., username/password, token, and the like) before the user is granted access to the secure portions of the website where account information is available. It should be appreciated that other types of secure resources (e.g., databases, files, software) are included within the scope of invention.

[0025] As described herein, instead of or in addition to traditional authentication credentials, the server computing device 106 receives a new type of credential: a video segment captured by the client device 102 (e.g., using camera device 103 coupled to client device 102). Because video segments are multifaceted (i.e., typically including visual and audio elements), they can advantageously be used to generate a video signature - that is, a collection of distinct visual and audio elements represented in the video segment that are used to identify the associated user and can be compared to other video segments submitted by the user to authenticate the user's identity and allow access to the system.

[0026] The request to access a secure resource includes the captured video segment which comprises a plurality of visual and audio elements. Continuing with the above example, upon reaching the login page of the financial institution's website, the client device 102 captures a video segment and transmits the video segment to the server computing device as part of the authentication process. In some embodiments, the video segment is a single frame (i.e., image) or set of frames of video data captured by the camera device 103 that is used by the server computing device 106 to authenticate the user and/or the client device 102. The video segment can include any number of visual and audio elements that, when analyzed together, comprise the video signature for the video segment.

[0027] FIG. 4 is a diagram of an exemplary video segment 400 to be analyzed to generate a video signature, according to an embodiment of the invention. As shown in FIG. 4, the video segment comprises a video of the user wearing a

Thales Exhibit 2001, Page 116 of 339
Okta v. Thales DIS France - IPR2026-00278

baseball cap 402, holding a cat 404, saying the word "Rosebud" 406, with a potted plant 408 in the corner of the room. Each of the visual and audio elements 402, 404, 406 and 408 are used by the system 100 during the video signature authentication process. In addition, other elements of the video segment can be used for authentication, such as the user himself, apparel that the user is wearing, elements of the room (e.g., door, window), and so forth. For example, the module 108 can use facial recognition techniques to analyze the user and the result of such facial recognition methodology can be used as part of the total score for the video segment (as described in greater detail below). Other examples include voice recognition technology to analyze the user's speech patterns, speech-to-text conversion technology to isolate audio cues and/or spoken words within the video segment, and motion detection technology to track movement of the user and/or objects within the scene of the video segment. For example, if the user nods his head during the video segment, the module 108 can analyze the speed, position, and timing of the head movement as part of the overall analysis process described below.

[0028] Continuing with the method 300 of FIG. 3, the video signature authentication module 108 of server computing device 106 analyzes (304) one or more of the plurality of visual and audio elements 402, 404, 406, 408 in the first video segment 400 to determine a value associated with each of the one or more analyzed elements. As can be appreciated, the module 108 uses image and audio analysis algorithms / techniques to extract the various visual and audio elements from the video segment. For example, the module 108 can extract the shape of the baseball cap 402 from the video segment (or a single image of the video segment) and compare it to a database (e.g., database 110) of known shapes to determine a match. The module 108 can also analyze other characteristics associated with the visual and audio elements as part of the authentication process - such as color, position, and movement. For example, the module 108 determines that the baseball cap 402 is green and is positioned on top of the user's head.

[0029] Also, one or more of the visual and audio elements in the video segment can be assigned multiple values based upon different characteristics of the respective element. For example, the module 108 assigns the baseball cap a first value based upon its color (e.g., green) and assigns the baseball cap a second value based upon its position (e.g., on top of the user's head).

[0030] In some embodiments, the module 108 assigns a numeric value to each of the visual and audio elements 402, 404, 406, 408 represented in the video segment during the analysis step. Table One below depicts exemplary values assigned to each of the visual and audio elements 402, 404, 406 and 408:

TABLE ONE

Visual / Audio Element	Assigned Value
Baseball cap	10
Green baseball cap	15
Baseball cap on user's head	20
Cat	10
White cat	15
Holding cat in right hand	20
Saying "Rosebud"	25
Potted plant	10
Plant in back corner of room	20
TOTAL SCORE	145

[0031] After analyzing the video segment, the server computing device 106 calculates (306) a total score for the first video segment 400 based upon the value associated with each of the one or more analyzed elements. As shown in the table above, the total score for the video segment 400 is 145, based upon the summation of the individual visual and audio elements analyzed by the module 108. In some embodiments, certain visual and/or audio elements are weighted differently according to a predetermined security profile selected by the user and/or assigned by the module 108. For example, a financial institution may want to weigh the audio element 406 more heavily in the total score than a visual element (e.g., 408) because the institution can utilize speech recognition technology to identify the user with great precision (e.g., it may be harder for an impostor to duplicate a video segment that includes an audio element spoken by the user).

[0032] The module 108 stores the video segment and the associated values for each of the analyzed visual and audio elements in a database 110. The module 108 associates the stored data as a video signature for the particular user that

Thales Exhibit 2001, Page 117 of 339
Okta v. Thales DIS France - IPR2026-00278

submitted the video segment. Thus, the first time a video segment is submitted for analysis by client device 102, the module 108 stores the video segment and associated values as the video signature against which future video segment submissions from the user / client device are compared, similar to a username / password combination provided by a user.

[0033] When a user subsequently attempts to authenticate and gain access to a secure resource after providing a video segment, the module 108 compares (308) the total score for the earlier-provided video segment (i.e., the video segment that has been analyzed and stored by the system as described above) to a score associated with a second video segment associated with the client device 102 and/or user in order to identify and authenticate the user. For example, during a subsequent request to authenticate to the server computing device 106 and access a secure resource, the client device 102 submits a new video segment which is then analyzed by the module 108 (as previously described). In order to successfully authenticate, the total score of the newly-submitted video segment as calculated by the module 108 meets or exceeds a predetermined threshold when compared to the previously-stored video segment (e.g., segment 400).

[0034] FIG. 5 is a diagram of an exemplary video segment 500 to be authenticated using a video signature, according to an embodiment of the invention. As shown in FIG. 5, the same user from FIG. 4 is present in the video segment. The video segment 500 includes a plurality of video and audio elements 502, 504, 506, 508: the user has an orange baseball cap 502 on top of his head, is holding a white cat 504 in his right hand, and is speaking the word "Roseburg" 506. Also, a potted plant 508 is positioned in the rear corner of the room.

[0035] The module 108 receives the video segment 500 from the client device 102 and analyzes the video segment 500 in the same manner as described previously. For example, the module 108 assigns a numeric value to each of the visual and audio elements 502, 504, 506, 508 represented in the video segment 500. During this process, the values assigned to the elements 502, 504, 506, 508 are further scaled by comparing them to the same elements 402, 404, 406, 408 as analyzed in the previously-stored video segment 400. Table Two below depicts exemplary values assigned to each of the visual and audio elements 502, 504, 506 and 508 and compared to the values previously assigned to the elements 402, 404, 406, 408 from the first video segment 400:

TABLE TWO

Visual / Audio Element (Second Video Segment)	Assigned Value	Visual / Audio Element (First Video Segment)	Assigned Value
Baseball cap	10	Baseball cap	10
Orange baseball cap	0	Green baseball cap	15
Baseball cap on user's head	20	Baseball cap on user's head	20
Cat	10	Cat	10
White cat	15	White cat	15
Holding cat in right hand	20	Holding cat in right hand	20
Saying "Roseburg"	10	Saying "Rosebud"	25
Potted plant	10	Potted plant	10
Plant in back corner of room	20	Plant in back corner of room	20
TOTAL SCORE	115	TOTAL SCORE	145

[0036] The module 108 determines a total score for the second video segment 500 to be one-hundred fifteen. The total score for the second video segment 500 is lower than the score for the previously-stored video segment 400 due to two main differences: a) the user is wearing an orange baseball cap, not a green cap; and b) the user is speaking the word "Roseburg" instead of "Rosebud." The differences result in the module 108 assigning a lower value to those two elements of the second video segment 500 (i.e., because they do not match the same characteristics of the elements as represented in the first video segment 400).

[0037] The module 108 determines (310) whether access to the secure resource is permitted based upon the comparison step. As shown in the table above, the module 108 determines that the total score for the second video segment 500 is within thirty points of the total score for the first video segment 400 (i.e., one-hundred fifteen to one-hundred forty-five). As a result, the module 108 can determine that the total score for the second segment 500 is sufficient to satisfy a predetermined threshold for permitting access to the secure resource. For example, the module 108 may determine that any total score for a submitted video segment that exceeds one hundred is sufficient to permit access.

[0038] In some embodiments, the user can provide certain scoring parameters or thresholds that provide some flexibility

Thales Exhibit 2001, Page 118 of 339
Okta v. Thales DIS France - IPR2026-00278

in the visual and audio elements required to be present in video segments submitted for authentication. For example, the user may prefer that the color of the baseball cap 402 is not used during the analysis and authentication process - so that he can wear any baseball cap he might have available and still be able to authenticate to the system.

[0039] In some embodiments, the module 108 evaluates each of the visual and audio elements individually as part of the determination process to calculate a deviation value for the respective elements. For example, the module 108 may determine that, because only two of the nine values for the visual and audio elements in the second video segment 500 fall more than ten points below the corresponding elements in the first video segment 400 (i.e., a deviation value of ten), the second video segment 500 is sufficient to authenticate the user / client device 102. In another example, the module 108 may require that every visual and audio element in the second video segment 500 fall within at least eight points of the corresponding element in the first video segment 400 in order to permit access to the secure resource. Table Three below depicts exemplary values assigned to each of the visual and audio elements 502, 504, 506 and 508 and compared to the values previously assigned to the elements 402, 404, 406, 408 from the first video segment 400, including a deviation value for each element comparison:

TABLE THREE

Visual / Audio Element (Second Video Segment)	Assigned Value	Visual / Audio Element (First Video Segment)	Assigned Value	Deviation Value
Baseball cap	10	Baseball cap	10	0
Orange baseball cap	0	Green baseball cap	15	15
Baseball cap on user's head	20	Baseball cap on user's head	20	0
Cat	10	Cat	10	0
White cat	15	White cat	15	0
Holding cat in right hand	20	Holding cat in right hand	20	0
Saying "Roseburg"	10	Saying "Rosebud"	25	15
Potted plant	10	Potted plant	10	0
Plant in back corner of room	20	Plant in back corner of room	20	0
TOTAL SCORE	115	TOTAL SCORE	145	

[0040] The aggregate deviation value between the elements of the two video segments is thirty, while the average deviation value is 3.33. In some examples, the module 108 can use the average deviation value to determine whether access to the secure resource is permitted while in other examples, the aggregated deviation value can be used. As can be appreciated, a variety of scoring and comparison techniques can be used without departing from the scope of the invention.

[0041] FIG. 6 is a diagram of another exemplary video segment 600 to be authenticated using a video signature, according to an embodiment of the invention. As shown in FIG. 6, the third video segment 600 includes a plurality of video and audio elements 604, 606, 608: a person is holding a white cat 604 in his left hand and is speaking the words "Play it again" 606. Also, a coat rack 608 is positioned in the rear comer of the room. The person in FIG. 6 is not wearing a hat.

[0042] The module 108 receives the third video segment 600 from the client device 102 and analyzes the video segment 600 in the same manner as described previously. For example, the module 108 assigns a numeric value to each of the visual and audio elements 604, 606, 608 represented in the video segment 600. During this process, the values assigned to the elements 604, 606, 608 are further scaled by comparing them to the same elements 402, 404, 406, 408 as analyzed in the previously-stored video segment 400. Table Four below depicts exemplary values assigned to each of the visual and audio elements 604, 606, 608 in video segment 600 and compared to the values previously assigned to the elements 402, 404, 406, 408 from the first video segment 400:

TABLE FOUR

Visual / Audio Element (Third Video Segment)	Assigned Value	Visual / Audio Element (First Video Segment)	Assigned Value
No baseball cap	0	Baseball cap	10
No baseball cap	0	Green baseball cap	15

Thales Exhibit 2001, Page 119 of 339
Okta v. Thales DIS France - IPR2026-00278

(continued)

Visual / Audio Element (Third Video Segment)	Assigned Value	Visual / Audio Element (First Video Segment)	Assigned Value
No baseball cap	0	Baseball cap on user's head	20
Cat	10	Cat	10
White cat	15	White cat	15
Holding cat in left hand	5	Holding cat in right hand	20
Saying "Play it again"	0	Saying "Rosebud"	25
Coat rack	0	Potted plant	10
Coat rack in back corner of room	5	Plant in back corner of room	20
TOTAL SCORE	35	TOTAL SCORE	145

[0043] The module 108 determines a total score for the third video segment 600 to be thirty-five. The total score for the third video segment 600 is significantly lower than the score for the previously-stored video segment 400 due to many differences between the two segments: a) the absence of a baseball cap, b) the cat positioned in the wrong hand, c) the person speaking the wrong phrase, and d) the wrong object being positioned in the corner of the room. In this example, an impostor may be trying to gain access to the secure resource by attempting to pass himself off as the user by submitting a fraudulent video segment (just as someone may attempt to learn a user's password by making attempts using random character strings). Because the total score for the third video segment 600 is far below the total score for the first video segment 400, the module 108 denies the request to access the secure resource and does not authenticate the person / client device 102 to the system.

[0044] In some embodiments, if the submitted video segment does not meet or exceed a predetermined threshold for permitting access to the secure resource, the module 108 can offer other authentication means to the user so that such access may be granted. For example, the module 108 can prompt the user and/or client device 102 for an auxiliary authentication credential (e.g., biometric information, device footprint, token, public/private key information, and the like) in order to verify the identity of the user.

[0045] The above-described techniques can be implemented in digital and/or analog electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. The implementation can be as a computer program product, i.e., a computer program tangibly embodied in a machine-readable storage device, for execution by, or to control the operation of, a data processing apparatus, e.g., a programmable processor, a computer, and/or multiple computers. A computer program can be written in any form of computer or programming language, including source code, compiled code, interpreted code and/or machine code, and the computer program can be deployed in any form, including as a stand-alone program or as a subroutine, element, or other unit suitable for use in a computing environment. A computer program can be deployed to be executed on one computer or on multiple computers at one or more sites.

[0046] Method steps can be performed by one or more processors executing a computer program to perform functions of the invention by operating on input data and/or generating output data. Method steps can also be performed by, and an apparatus can be implemented as, special purpose logic circuitry, e.g., a FPGA (field programmable gate array), a FPAA (field-programmable analog array), a CPLD (complex programmable logic device), a PSoC (Programmable System-on-Chip), ASIP (application-specific instruction-set processor), or an ASIC (application-specific integrated circuit), or the like. Subroutines can refer to portions of the stored computer program and/or the processor, and/or the special circuitry that implement one or more functions.

[0047] Processors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and any one or more processors of any kind of digital or analog computer. Generally, a processor receives instructions and data from a read-only memory or a random access memory or both. The essential elements of a computer are a processor for executing instructions and one or more memory devices for storing instructions and/or data. Memory devices, such as a cache, can be used to temporarily store data. Memory devices can also be used for long-term data storage. Generally, a computer also includes, or is operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data, e.g., magnetic, magneto-optical disks, or optical disks. A computer can also be operatively coupled to a communications network in order to receive instructions and/or data from the network and/or to transfer instructions and/or data to the network. Computer-readable storage mediums suitable for embodying computer program instructions and data include all forms of volatile and non-volatile memory, including by way of example semiconductor memory devices, e.g., DRAM, SRAM, EPROM, EEPROM, and flash memory devices; magnetic disks, e.g., internal hard disks or removable disks; magneto-optical disks; and optical

Thales Exhibit 2001, Page 120 of 339
Okta v. Thales DIS France - IPR2026-00278

disks, e.g., CD, DVD, HD-DVD, and Blu-ray disks. The processor and the memory can be supplemented by and/or incorporated in special purpose logic circuitry.

[0048] To provide for interaction with a user, the above described techniques can be implemented on a computing device in communication with a display device, e.g., a CRT (cathode ray tube), plasma, or LCD (liquid crystal display) monitor, a mobile device display or screen, a holographic device and/or projector, for displaying information to the user and a keyboard and a pointing device, e.g., a mouse, a trackball, a touchpad, or a motion sensor, by which the user can provide input to the computer (e.g., interact with a user interface element). Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback, e.g., visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic, speech, and/or tactile input.

[0049] The above described techniques can be implemented in a distributed computing system that includes a back-end component. The back-end component can, for example, be a data server, a middleware component, and/or an application server. The above described techniques can be implemented in a distributed computing system that includes a front-end component. The front-end component can, for example, be a client computer having a graphical user interface, a Web browser through which a user can interact with an example implementation, and/or other graphical user interfaces for a transmitting device. The above described techniques can be implemented in a distributed computing system that includes any combination of such back-end, middleware, or front-end components.

[0050] The components of the computing system can be interconnected by transmission medium, which can include any form or medium of digital or analog data communication (e.g., a communication network). Transmission medium can include one or more packet-based networks and/or one or more circuit-based networks in any configuration. Packet-based networks can include, for example, the Internet, a carrier internet protocol (IP) network (e.g., local area network (LAN), wide area network (WAN), campus area network (CAN), metropolitan area network (MAN), home area network (HAN)), a private IP network, an IP private branch exchange (IPBX), a wireless network (e.g., radio access network (RAN), Bluetooth, Wi-Fi, WiMAX, 3G, 4G, 4G LTE, 5G, general packet radio service (GPRS) network, HiperLAN), and/or other packet-based networks. Circuit-based networks can include, for example, the public switched telephone network (PSTN), a legacy private branch exchange (PBX), a wireless network (e.g., RAN, code-division multiple access (CDMA) network, time division multiple access (TDMA) network, global system for mobile communications (GSM) network), and/or other circuit-based networks.

[0051] Information transfer over transmission medium can be based on one or more communication protocols. Communication protocols can include, for example, Ethernet protocol, Internet Protocol (IP), Voice over IP (VOIP), a Peer-to-Peer (P2P) protocol, Hypertext Transfer Protocol (HTTP), Session Initiation Protocol (SIP), H.323, Media Gateway Control Protocol (MGCP), Signaling System #7 (SS7), a Global System for Mobile Communications (GSM) protocol, a Push-to-Talk (PTT) protocol, a PTT over Cellular (POC) protocol, Universal Mobile Telecommunications System (UMTS), 3GPP Long Term Evolution (LTE) and/or other communication protocols.

[0052] Devices of the computing system can include, for example, a computer, a computer with a browser device, a telephone, an IP phone, a mobile device (e.g., cellular phone, personal digital assistant (PDA) device, smart phone, tablet, laptop computer, electronic mail device), and/or other communication devices. The browser device includes, for example, a computer (e.g., desktop computer and/or laptop computer) with a World Wide Web browser (e.g., Chrome™ from Google, Inc., Microsoft® Internet Explorer® available from Microsoft Corporation, and/or Mozilla® Firefox available from Mozilla Corporation). Mobile computing device include, for example, a Blackberry® from Research in Motion, an iPhone® from Apple Corporation, and/or an Android™-based device. IP phones include, for example, a Cisco® Unified IP Phone 7985G and/or a Cisco® Unified Wireless Phone 7920 available from Cisco Systems, Inc.

[0053] Comprise, include, and/or plural forms of each are open ended and include the listed parts and can include additional parts that are not listed. And/or is open ended and includes one or more of the listed parts and combinations of the listed parts.

[0054] One skilled in the art will realize the invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. The foregoing embodiments are therefore to be considered in all respects illustrative rather than limiting of the invention described herein.

Claims

1. A method for authentication using a video signature, the method comprising:

receiving, by a computing device from a remote device associated with a user, a request to access a secure resource, the request including a first video segment comprising a plurality of visual and audio elements, wherein at least a first one of the visual elements comprises a physical characteristic of the user, at least a second one of the visual elements comprises a physical object in proximity to the user, and at least a third one of the visual

Thales Exhibit 2001, Page 121 of 339
Okta v. Thales DIS France - IPR2026-00278

elements comprises an element of the environment surrounding the user;
determining, by the computing device, a plurality of characteristics associated with each of the plurality of visual and audio elements;
assigning, by the computing device, a value to each of the characteristics based upon predetermined value information stored by the computing device;
calculating, by the computing device, a total score for the first video segment based upon the value associated with each of the characteristics;
comparing, by the computing device, the total score for the first video segment to a score associated with a second video segment previously received from the remote device;
determining, by the computing device, whether to permit the remote device to access the secure resource based upon the comparison step; and
connecting, by the computing device, the remote device to the secure resource if access is permitted.

2. The method of claim 1, further comprising:

storing, by the computing device, the values for each of the characteristics in a database coupled to the computing device.

3. The method of claim 2, wherein the plurality of characteristics includes at least two of:

a position of a visual element, movement of a visual element, a color of a visual element, a type of a visual element, and an absence of a visual element.

4. The method of any preceding claim, further comprising performing, by the computing device, a speech-to-text conversion on an audio element.

5. The method of any preceding claim, wherein the values are assigned to the characteristics based upon frequency of appearance within frames of the first video segment.

6. The method of any preceding claim, wherein the predetermined value information is adjusted based upon preferences received from the remote device.

7. The method of any preceding claim, wherein the calculating step includes assigning, by the computing device, a weight to one or more of the characteristics based upon a security profile at the computing device.

8. The method of any preceding claim, the comparing step further comprising:

comparing, by the computing device, the value associated with one of the characteristics in the first video segment to a value associated with a corresponding characteristic of the same element in the second video segment; and
determining, by the computing device, a deviation value based upon the comparison of the characteristic values.

9. The method of claim 8, further comprising:

aggregating, by the computing device, the deviation value for the comparisons of each of the characteristic values; and
determining, by the computing device, whether the aggregated deviation value falls below a predetermined threshold.

10. The method of any preceding claim, wherein the plurality of visual and audio elements include a phrase spoken by the user.

11. The method of any preceding claim, wherein the first video segment is captured using a camera connected to the remote device.

12. The method of any preceding claim, wherein the remote device is a mobile device.

13. The method of any preceding claim, wherein the secure resource is a website.

Thales Exhibit 2001, Page 122 of 339
Okta v. Thales DIS France - IPR2026-00278

14. A system for authentication using a video signature, the system comprising a computing device configured to:

receive, from a remote device associated with a user, a request to access a secure resource, the request including a first video segment comprising a plurality of visual and audio elements, wherein at least a first one of the visual elements comprises a physical characteristic of the user, at least a second one of the visual elements comprises a physical object in proximity to the user, and at least a third one of the visual elements comprises an element of the environment surrounding the user;
determine a plurality of characteristics associated with each of the plurality of visual and audio elements;
assign a value to each of the characteristics based upon predetermined value information stored by the computing device;
calculate a total score for the first video segment based upon the value associated with each of the characteristics;
compare the total score for the first video segment to a score associated with a second video segment previously received from the remote device;
determine whether to permit the remote device to access the secure resource based upon the comparison step; and
connect the remote device to the secure resource if access is permitted.

15. The system of claim 14, wherein the computing device is further configured to:

store the values for each of the characteristics in a database coupled to the computing device.

16. The system of claim 14 or 15, wherein the first video segment is captured using a camera connected to the remote device.

17. The system of claim 14, 15 or 16, wherein the remote device is a mobile device.

18. A computer program product, tangibly embodied in a non-transitory computer readable storage medium, for authentication using a video signature, the computer program product including instructions operable to cause a computing device to: carry out a method according to any of claims 1 to 13.

Thales Exhibit 2001, Page 123 of 339
Okta v. Thales DIS France - IPR2026-00278

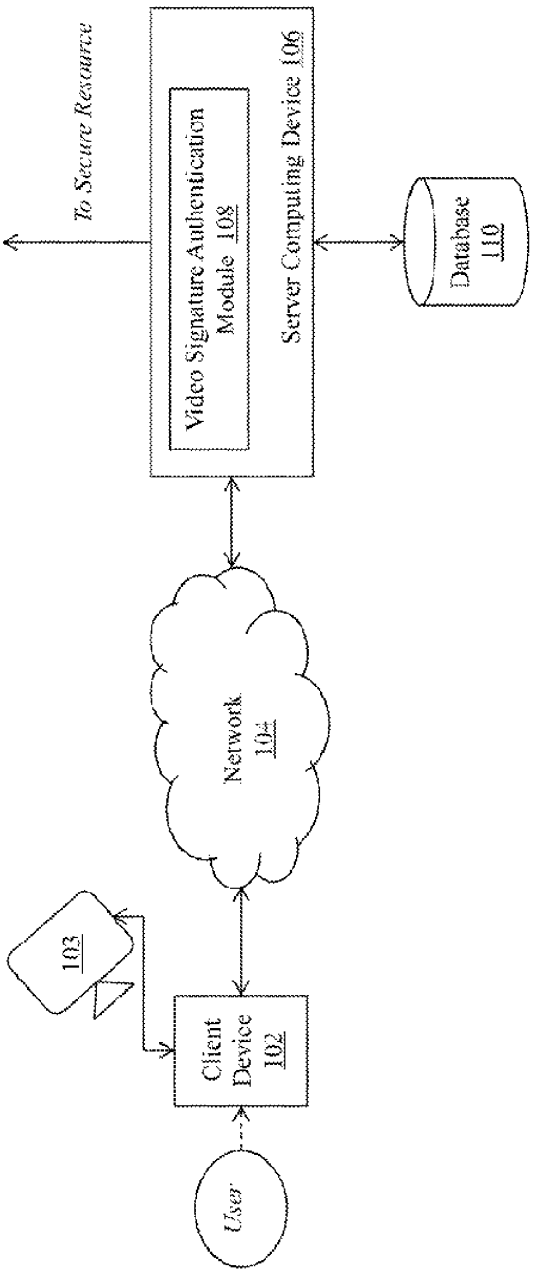


FIG. 1

Thales Exhibit 2001, Page 124 of 339
Okta v. Thales DIS France - IPR2026-00278

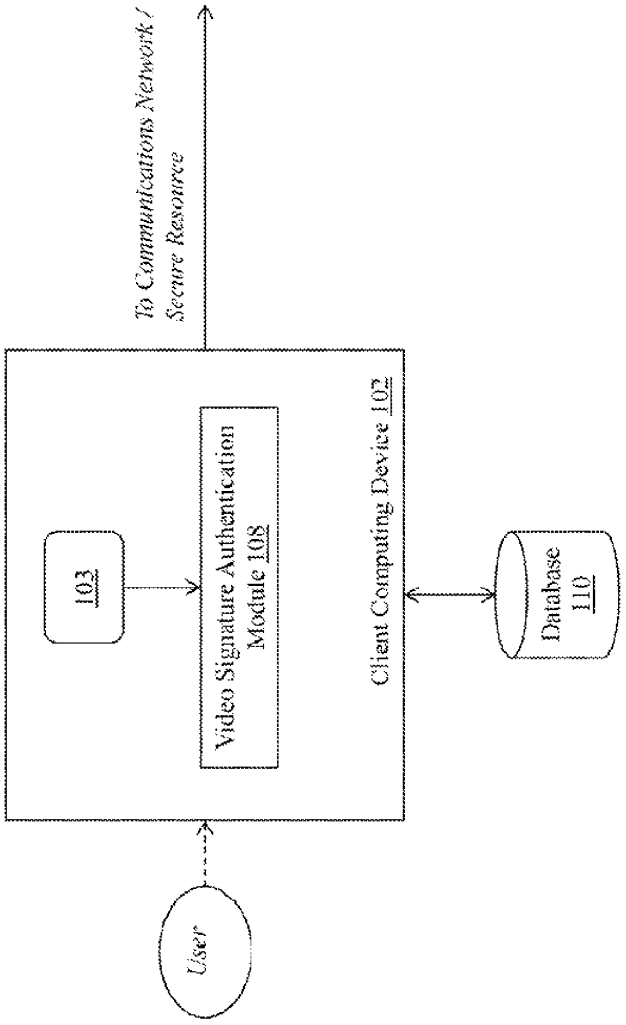


FIG. 2

Thales Exhibit 2001, Page 125 of 339
Okta v. Thales DIS France - IPR2026-00278

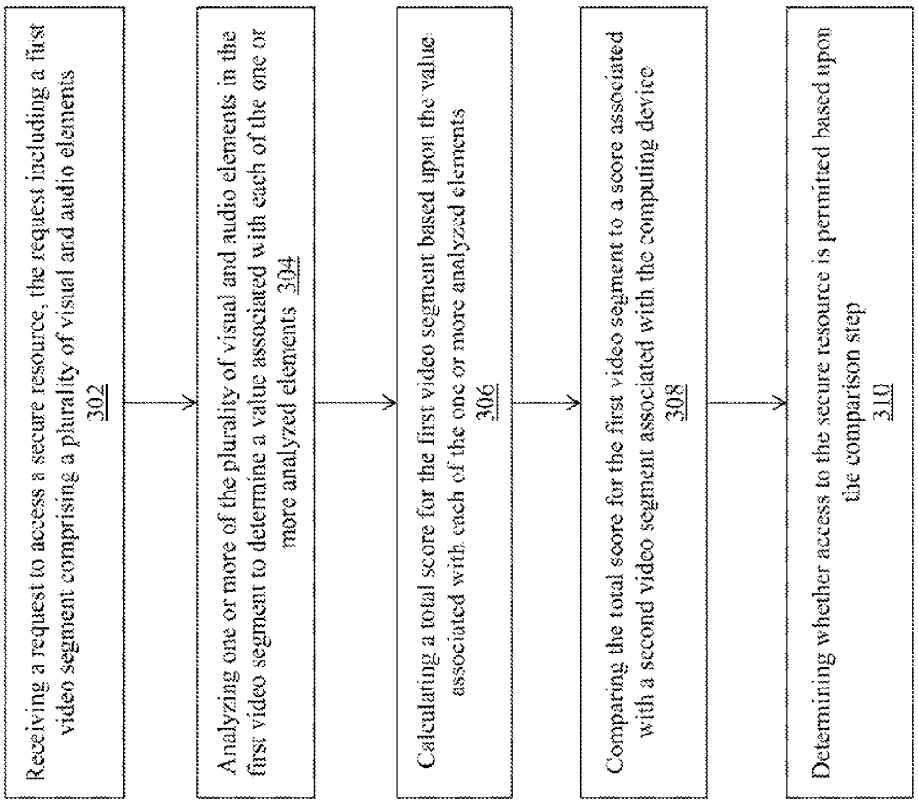


FIG. 3

Thales Exhibit 2001, Page 126 of 339
Okta v. Thales DIS France - IPR2026-00278

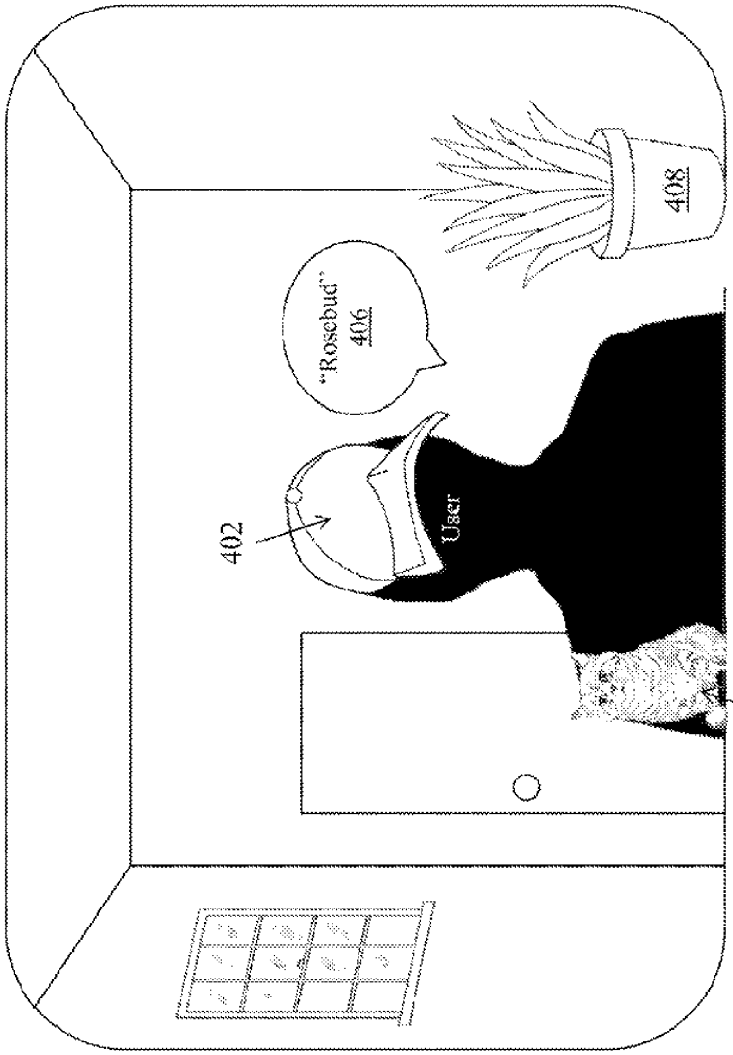


FIG. 4

Thales Exhibit 2001, Page 127 of 339
Okta v. Thales DIS France - IPR2026-00278

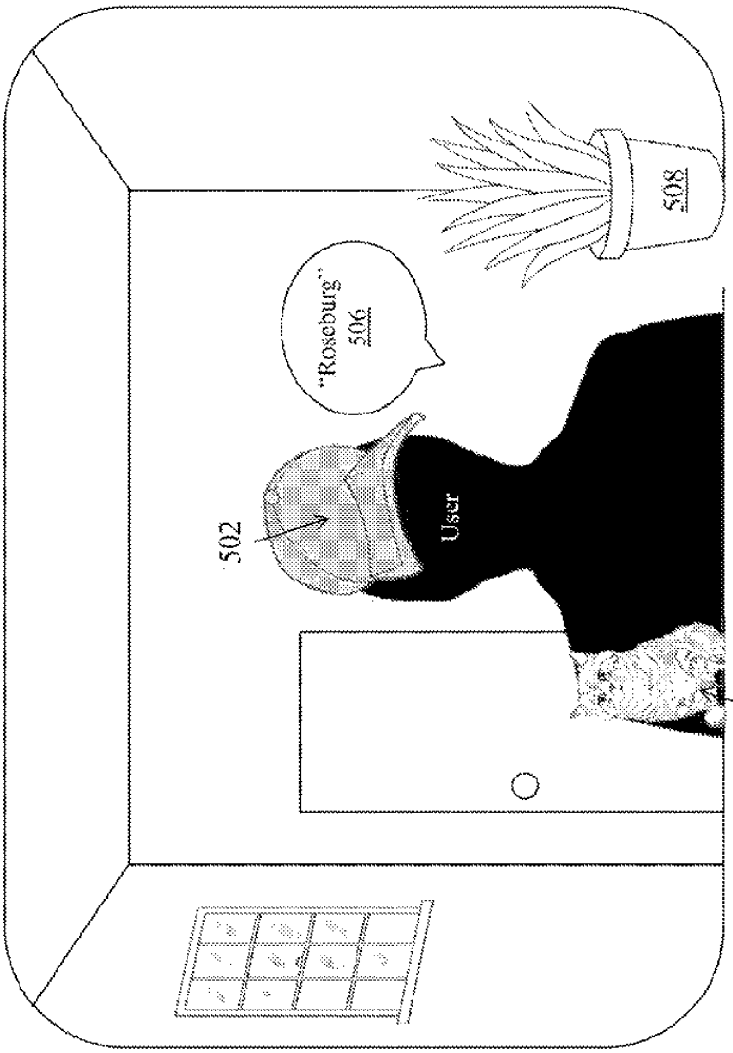


FIG. 5

Thales Exhibit 2001, Page 128 of 339
Okta v. Thales DIS France - IPR2026-00278

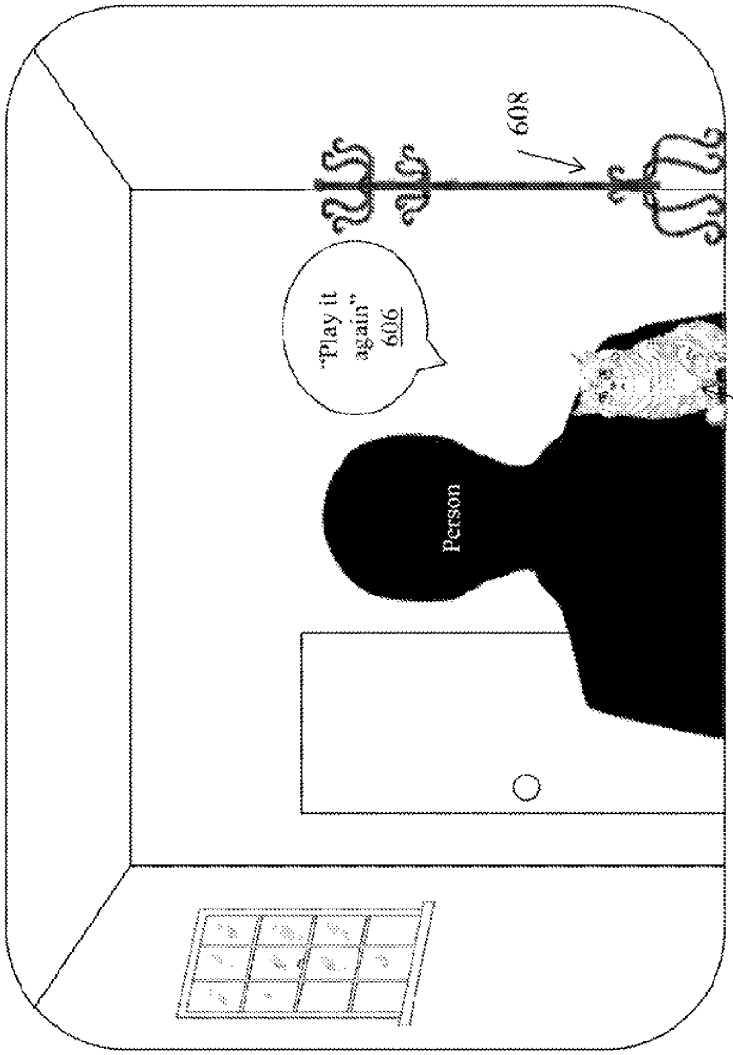


FIG. 6

Thales Exhibit 2001, Page 129 of 339
Okta v. Thales DIS France - IPR2026-00278

Espacenet

Bibliographic data: US2020336300 (A1) — 2020-10-22

AUTHENTICATION METHOD, DEVICE AND SYSTEM

Inventor(s): DELHOSTE FABRICE [FR]; PAILLART FRÉDÉRIC [FR]; PETIT SÉBASTIEN [FR] ± (DELHOSTE, Fabrice, ; PAILLART, Frédéric, ; PETIT, Sébastien)

Applicant(s): THALES DIS FRANCE SA [FR] ± (THALES DIS FRANCE SA)

Classification: - international: *H04L9/06; H04L9/08; H04L9/32*
- cooperative: **G06F21/44 (EP); H04L9/0643 (US); H04L9/0866 (US); H04L9/3231 (US); H04L9/3236 (EP); H04L9/3242 (US);** H04L9/0643 (EP)

Application number: US201816958252 20181119 Global Dossier

Priority number(s): EP20170306977 20171229 ; WO2018EP81759 20181119

Also published as: EP3506138 (A1) EP3732600 (A1) WO2019129422 (A1)

Abstract of US2020336300 (A1)

The invention relates to an authentication method. The method comprises: collecting, based on a predetermined authentication policy, at least one context data element; constituting, based on the at least one collected context data element, a data packet; generating, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash; sending the generated hash; generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and authenticating successfully or not based on the generated hash distance, as an authentication step. The invention also relates to corresponding device and system.

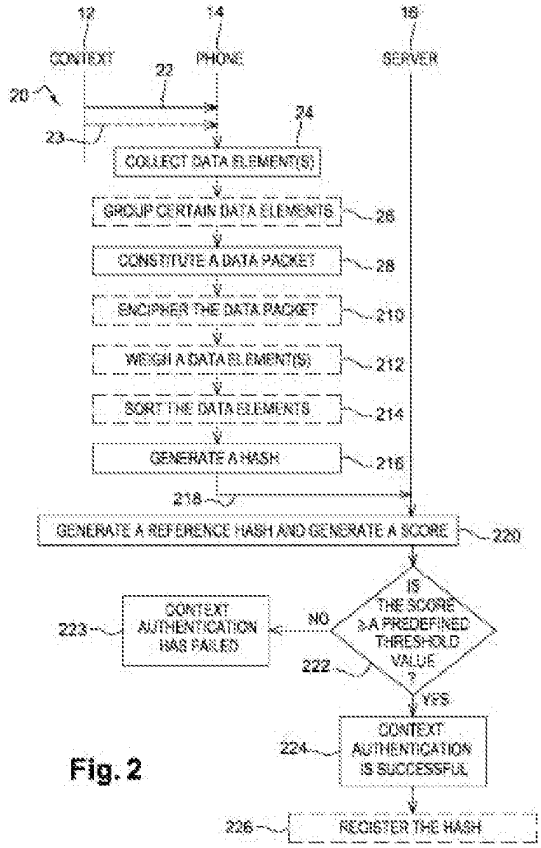


Fig. 2

Thales Exhibit 2001, Page 131 of 339
Okta v. Thales DIS France - IPR2026-00278

Bibliographic Data

Application No: 16/958,252

Foreign Priority claimed: (•) Yes ( ) No

35 USC 119 (a-d) conditions met: [✓] Yes [ ] No [ ] Met After Allowance

Verified and Acknowledged: /MAYASA A. SHAAWAT/ Examiner's Signature [ ] Initials

Title: AUTHENTICATION METHOD, DEVICE AND SYSTEM

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
06/26/2020	713	2433	1032326-001016
RULE			

APPLICANTS

THALES DIS FRANCE SA, Meudon, FRANCE

INVENTORS

Fabrice DELHOSTE, Gemenos, FRANCE

Frédéric PAILLART, Gemenos, FRANCE

Sébastien PETIT, Gemenos, FRANCE

CONTINUING DATA

This application is a 371 of PCT/EP2018/081759 11/19/2018

FOREIGN APPLICATIONS

EPO EP17306977.4 12/29/2017

IF REQUIRED, FOREIGN LICENSE GRANTED**

07/15/2020

STATE OR COUNTRY

FRANCE

ADDRESS

BUCHANAN, INGERSOLL & ROONEY PC
1737 KING STREET
SUITE 500
ALEXANDRIA, VA 22314-2727
UNITED STATES

FILING FEE RECEIVED

$2,180

Based on USPTO Form PTO/SB/08

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Fabrice DELHOSTE
	Art Unit	
	Examiner Name	
	Attorney Docket Number	1032326-001016

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	20170109514	A1	2017-04-20	Cheng, et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2924603	EP	A2	2015-09-30	FMR LLC		☐
	2	2016083216	WO	A1	2016-06-02	GEMALTO SA		☐

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	International Search Report (PCT/ISA/210) and Written Opinion (PCT/ISA/237) mailed on January 22, 2019, by the European Patent Office as the International Searching Authority for International Application No. PCT/EP2018/081759.	☐

EXAMINER SIGNATURE

Examiner Signature	/MAYASA A. SHAAWAT/	Date Considered	09/07/2021

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.A.S./

Based on USPTO Form PTO/SB/08

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Fabrice DELHOSTE
	Art Unit	
	Examiner Name	
	Attorney Docket Number	1032326-001016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document.
[4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e) (1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e) (2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James A LaBarre/	Date (YYYY-MM-DD)	2020-06-26
Name/Print	James A. LaBarre	Registration Number	28,632

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.A.S./

Based on USPTO Form PTO/SB/08

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Fabrice DELHOSTE
	Art Unit	
	Examiner Name	
	Attorney Docket Number	1032326-001016

require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.A.S./

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	16958252
Filing Date	2020-06-26
First Named Inventor	Fabrice DELHOSTE et al.
Art Unit	OPAP
Examiner Name	CENTRAL, DOCKET
Attorney Docket Number	1032326-001016

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	9594906	B1	2017-03-14	LANGTON et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20150096023	A1	2015-04-02	MESDAQ et al.	
	2	20160323243	A1	2016-11-03	LEVASSEUR et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.A.S./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16958252
	Filing Date	2020-06-26
	First Named Inventor	Fabrice DELHOSTE et al.
	Art Unit	OPAP
	Examiner Name	CENTRAL, DOCKET
	Attorney Docket Number	1032326-001016

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Office Action (Communication pursuant to Article 94(3) EPC) issued on July 6, 2021, by the European Patent Office in corresponding European Patent Application No. 18800679.5. (2 pages)	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/MAYASA A. SHAAWAT/	Date Considered	09/07/2021

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.A.S./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16958252
	Filing Date	2020-06-26
	First Named Inventor	Fabrice DELHOSTE et al.
	Art Unit	OPAP
	Examiner Name	CENTRAL, DOCKET
	Attorney Docket Number	1032326-001016

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

✓ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James A LaBarre/	Date (YYYY-MM-DD)	2021-07-28
Name/Print	James A. LaBarre	Registration Number	28632

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.A.S./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.A.S./

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	16958252
	Filing Date	2020-06-26
	First Named Inventor	Fabrice DELHOSTE et al.
	Art Unit	OPAP
	Examiner Name	CENTRAL, DOCKET
	Attorney Docket Number	1032326-001016

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	9594906	B1	2017-03-14	LANGTON et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20150096023	A1	2015-04-02	MESDAQ et al.	
	2	20160323243	A1	2016-11-03	LEVASSEUR et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16958252
	Filing Date	2020-06-26
	First Named Inventor	Fabrice DELHOSTE et al.
	Art Unit	OPAP
	Examiner Name	CENTRAL, DOCKET
	Attorney Docket Number	1032326-001016

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Office Action (Communication pursuant to Article 94(3) EPC) issued on July 6, 2021, by the European Patent Office in corresponding European Patent Application No. 18800679.5. (2 pages)	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	16958252
	Filing Date	2020-06-26
	First Named Inventor	Fabrice DELHOSTE et al.
	Art Unit	OPAP
	Examiner Name	CENTRAL, DOCKET
	Attorney Docket Number	1032326-001016

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

✓ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James A LaBarre/	Date (YYYY-MM-DD)	2021-07-28
Name/Print	James A. LaBarre	Registration Number	28632

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	43363086
Application Number:	16958252
International Application Number:	
Confirmation Number:	5318
Title of Invention:	AUTHENTICATION METHOD, DEVICE AND SYSTEM
First Named Inventor/Applicant Name:	Fabrice DELHOSTE
Customer Number:	21839
Filer:	James A. LaBarre/Kevin Chanthakhoune
Filer Authorized By:	James A. LaBarre
Attorney Docket Number:	1032326-001016
Receipt Date:	28-JUL-2021
Filing Date:	26-JUN-2020
Time Stamp:	12:05:41
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	PTO_SB08.pdf	1035072 252fe7152fab53688e89319519c72fa6e348ae54	no	4
Warnings:					

Information:					
2	Other Reference-Patent/App/Search documents	EPOA_07062021.pdf	206278 5eb7a3eac522ab6bd6684005eae2742eae41a6af	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	1241350	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

506457276 01/20/2021

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
Stylesheet Version v1.2

EPAS ID: PAT6504048

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	ASSIGNMENT

CONVEYING PARTY DATA

Name	Execution Date
FABRICE DELHOSTE	08/24/2020
FREDERIC PAILLART	01/11/2021
SEBASTIEN PETIT	08/24/2020

RECEIVING PARTY DATA

Name:	THALES DIS FRANCE SA
Street Address:	6, RUE DE LA VERRERIE
City:	MEUDON
State/Country:	FRANCE
Postal Code:	92190

PROPERTY NUMBERS Total: 1

Property Type	Number
Application Number:	16958252

CORRESPONDENCE DATA

Fax Number: (703)836-7419

Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.

Phone: 7038366620
Email: ann.elkins@bipc.com
Correspondent Name: BUCHANAN INGERSOLL & ROONEY PC
Address Line 1: 1737 KING STREET
Address Line 2: SUITE 500
Address Line 4: ALEXANDRIA, VIRGINIA 22314

ATTORNEY DOCKET NUMBER:	1032326-001016
NAME OF SUBMITTER:	ANN ELKINS
SIGNATURE:	/Ann Elkins/
DATE SIGNED:	01/20/2021
	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 2
source=1032326_1016_ExCombDeclAssign#page1.tif
source=1032326_1016_ExCombDeclAssign#page2.tif

Attorney Docket No._____

COMBINED DECLARATION AND ASSIGNMENT (JOINT)

As one of the below named inventors, I hereby declare that this Combined Declaration and Assignment is directed to:

(1) U.S. application number or PCT application number 16/958,252
filed on November 19 2018
entitled AUTHENTICATION METHOD, DEVICE AND SYSTEM

or

(2) the attached application entitled

DECLARATION

As one of the below named inventors, I further declare that:

The above-identified application was made or authorized to be made by me.

I believe that I am an original joint inventor of a claimed invention in the application.

I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

ASSIGNMENT

THIS ASSIGNMENT, by the undersigned inventors (hereinafter referred to as "the Assignors"), respectively, witnesseth:

WHEREAS, the Assignors have invented certain new and useful improvements set forth in an application for Letters Patent of the United States, which is a nonprovisional application;

WHEREAS, THALES DIS FRANCE SA , a corporation duly organized under and pursuant to the laws of FRANCE and having a principal place of business at:

6, rue de la Verrerie - 92190 MEUDON - FRANCE

(hereinafter referred to as "the Assignee"), is desirous of acquiring the entire right, title, and interest in and to said inventions, the right to file applications on said inventions and the entire right, title and interest in and to any applications, including provisional applications for Letters Patent of the United States or other countries claiming priority to said application, and in and to any Letters Patent or Patents, United States or foreign, to be obtained therefor and thereon.

Thales Exhibit 2001, Page 147 of 339
Okta v. Thales DIS France - IPR2026-00278

NOW, THEREFORE, for good and sufficient consideration, the receipt of which is hereby acknowledged, the Assignors have sold, assigned, transferred, and set over, and by these presents do sell, assign, transfer, and set over, unto the Assignee, its successors, legal representatives, and assigns the entire right, title, and interest in and to the above-mentioned inventions, the right to file applications on said inventions and the entire right, title and interest in and to any applications for Letters Patent of the United States or other countries claiming priority to said applications, and any and all Letters Patent or Patents of the United States of America and all foreign countries that may be granted therefor and thereon, and in and to any and all applications claiming priority to said applications, divisions, continuations, and continuations-in-part of said applications, and reissues and extensions of said Letters Patent or Patents, and all rights under the International Convention for the Protection of Industrial Property, the same to be held and enjoyed by the Assignee, for its own use and behoof and the use and behoof of its successors, legal representatives, and assigns, to the full end of the term or terms for which Letters Patent or Patents may be granted as fully and entirely as the same would have been held and enjoyed by the Assignors had this sale and assignment not been made;

AND for the same consideration, the Assignors hereby covenant and agree to and with the Assignee, its successors, legal representatives, and assigns, that, at the time of execution and delivery of these presents, the Assignors are the sole and lawful owners of the entire right, title, and interest in and to the inventions set forth in said applications and said applications, including provisional applications, above-mentioned, and that the same are unencumbered, and that the Assignors have good and full right and lawful authority to sell and convey the same in the manner herein set forth;

AND for the same consideration, the Assignors hereby covenant and agree to and with the Assignee, its successors, legal representatives, and assigns that the Assignors will, whenever counsel of the Assignee, or the counsel of its successors, legal representatives, and assigns, shall advise that any proceeding in connection with said inventions or said applications for Letters Patent or Patents, or any proceeding in connection with Letters Patent or Patents for said inventions in any country, including interference proceedings, is lawful and desirable, or that any application claiming priority to said application, division, continuation, or continuation-in-part of any applications for Letters Patent or Patents, or any reissue or extension of any Letters Patent or Patents to be obtained thereon, is lawful and desirable, sign all papers and documents, take all lawful oaths, and do all acts necessary or required to be done for the procurement, maintenance, enforcement, and defense of Letters Patent or Patents for said inventions, without charge to the Assignee, its successors, legal representatives, and assigns, but at the cost and expense of the Assignee, its successors, legal representatives, and assigns;

AND the Assignors hereby request the Commissioner of Patents to issue any and all said Letters Patent of the United States to the Assignee as the Assignee of said inventions, the Letters Patent to be issued for the sole use and behoof of the Assignee, its successors, legal representatives, and assigns.

Date	Name	Signature
24/08/20	DELHOSTE, Fabrice	
11/01/2021	PAILLART, Frédéric	
24/08/20	PETIT, Sébastien	

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/958,252	06/26/2020	Fabrice DELHOSTE	1032326-001016

CONFIRMATION NO. 5318

21839
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

PUBLICATION NOTICE

OC00000120836739

Title:AUTHENTICATION METHOD, DEVICE AND SYSTEM

Publication No.US-2020-0336300-A1
Publication Date:10/22/2020

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET Substitute for Form PTO-1360 (For use with Form PTO/SB/06)	Application Number 16958252	Filing Date
	Applicant(s) Fabrice DELHOSTE	
	* May be used for additional claims or amendments	

CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT	
	Indep	Depend	Indep	Depend	Indep	Depend
1	1		---	---		
2		1	---	---		
3		2	---	---		
4		(1)	---	---		
5		(1)	---	---		
6		(1)	---	---		
7		(1)	---	---		
8		(1)	---	---		
9		(1)	---	---		
10		(1)	---	---		
11		(1)	---	---		
12		(1)	---	---		
13	1		---	---		
14		1	---	---		
15	1		---	---		
16			1			
17				1		
18				1		
19				1		
20				1		
21				1		
22				1		
23			1			
24			1			
25			1			
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						
48						
49						
50						
Total Indep	3		4		0	
Total Depend	13	↵	6	↵	0	↵
Total Claims	16		10		0	

	*		*		*	
	Indep	Depend	Indep	Depend	Indep	Depend
51						
52						
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						
70						
71						
72						
73						
74						
75						
76						
77						
78						
79						
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						
98						
99						
100						

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
16/958,252	06/26/2020		2180	1032326-001016	10	4

CONFIRMATION NO. 5318

21839
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

FILING RECEIPT

OC000000118486449

Date Mailed: 07/16/2020

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Fabrice DELHOSTE, Gemenos, FRANCE;
Frédéric PAILLART, Gemenos, FRANCE;
Sébastien PETIT, Gemenos, FRANCE;

Applicant(s)

THALES DIS FRANCE SA, Meudon, FRANCE;

Assignment For Published Patent Application

THALES DIS FRANCE SA, Meudon, FRANCE

Power of Attorney: The patent practitioners associated with Customer Number 21839

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/EP2018/081759 11/19/2018

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)
EUROPEAN PATENT OFFICE (EPO) 17306977.4 12/29/2017

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Thales Exhibit 2001, Page 151 of 339
Okta v. Thales DIS France - IPR2026-00278

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 07/15/2020
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 16/958,252**
Projected Publication Date: 10/22/2020
Non-Publication Request: No
Early Publication Request: No
Title

AUTHENTICATION METHOD, DEVICE AND SYSTEM

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

U.S. APPLICATION NO.	FIRST NAMED INVENTOR	ATTY. DOCKET NO.
16/958,252	Fabrice DELHOSTE	1032326-001016

21839
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

INTERNATIONAL APPLICATION NO.	
PCT/EP2018/081759	
I.A. FILING DATE	PRIORITY DATE
11/19/2018	12/29/2017

CONFIRMATION NO. 5318
371 ACCEPTANCE LETTER

OC000000118486450

Date Mailed: 07/16/2020

NOTICE OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C 371 AND 37 CFR 1.495

The applicant is hereby advised that the United States Patent and Trademark Office, in its capacity as a Designated / Elected Office (37 CFR 1.495), has ACCEPTED the above identified international application for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above. A Filing Receipt will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE "FILING DATE or 371(c) DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 (c)(1) and (c)(2) REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN BELOW.** The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363)

06/26/2020
DATE OF RECEIPT OF 35 U.S.C.
371(c)(1) and (c)(2) REQUIREMENTS

The following items have been received:

- Copy of the International Application filed on 06/26/2020
- Copy of the International Search Report filed on 06/26/2020
- Preliminary Amendments filed on 06/26/2020
- Information Disclosure Statements filed on 06/26/2020
- U.S. Basic National Fees filed on 06/26/2020
- Assignee Statement for PGPUB filed on 06/26/2020
- Authorize Access to Search Results filed on 06/26/2020
- Priority Documents filed on 06/26/2020
- Power of Attorney filed on 06/26/2020
- Authorization to Permit Access filed on 06/26/2020
- Application Data Sheet (37 CFR 1.76) filed on 06/26/2020

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.495(c).

FORM PCT/DO/EO/903 (371 Acceptance Notice)

Thales Exhibit 2001, Page 154 of 339
Okta v. Thales DIS France - IPR2026-00278

- Properly executed inventor's oath or declaration for the following inventor(s) has not been submitted: **Fabrice DELHOSTE**, **Frédéric PAILLART**, and **Sébastien PETIT**

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

LESLIE R CHASE

Telephone: (703) 756-1026

FORM PCT/DO/EO/903 (371 Acceptance Notice)

Thales Exhibit 2001, Page 155 of 339
Okta v. Thales DIS France - IPR2026-00278

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 16/958,252

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	300
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	520
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	760
TOTAL CLAIMS (37 CFR 1.16(i))	10 minus 20 =	*			OR	x 100 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	* 1				x 460 =	460
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	2040

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

CLAIMS

1. An authentication method (20) comprising:

- collecting (24), based on a predetermined authentication policy, at least one context data element;
- constituting (28), based on the at least one collected context data element, a data packet;
- generating (216), by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- sending the generated hash;
- generating (220), as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and
- authenticating (224) successfully or not (223) based on the generated hash distance, as an authentication step.

2. Method according to claim 1, wherein, the predetermined hash type algorithm comprising a locality sensitive hash type algorithm, the method further comprises, as the hash distance generation step and the authentication step, the following steps:

- generating, by using the locality sensitive hash type algorithm, a score, as a level of similarity between the generated hash and the predetermined reference hash;
- comparing the score to a predetermined threshold value;
- authenticating successfully only if the score is equal to or greater than the predetermined threshold value.

3. Method according to claim 1 or 2, wherein, prior to generating the hash, the method further comprises sorting, according to a numerical order, the at least one collected context data element within the data packet.

4. Method according to any previous claim, wherein, prior to generating the hash, the method further comprises weighting, according to the authentication policy, at least one of the at least one context data element.

5. Method according to any previous claim, wherein, prior to constituting the data packet, the method further comprises grouping, according to the authentication policy,

together at least two context data elements comprised within the at least one context data element, to constitute at least one corresponding context data group.

6. Method according to any previous claim, wherein, prior to generating the hash, the method further comprises ciphering, according to the authentication policy, the data packet.

7. Method according to claim 6, wherein a key used for the data packet ciphering includes a key generated by using a hash-based message authentication code key type derivation function.

8. Method according to any previous claim, wherein the hash type algorithm includes at least one element of a group including:
- a locality sensitive hash type algorithm;
- a Trend micro Locality Sensitive Hash type algorithm;
- a nilsimsa type algorithm;
- an sdhash type algorithm;
- an ssdeep type algorithm; and
- a fuzzy matching type algorithm;
- an approximate matching type algorithm;
- a near duplicate matching type algorithm; and
- a similarity detection type algorithm.

9. Method according to any previous claim, wherein, each time the authentication is successful, the method further comprises storing the generated hash.

10. Method according to any previous claim, wherein, each time the authentication is successful, the method further comprises registering, instead of the predetermined reference hash, the generated hash, as an updated reference hash to be used for a next authentication.

11. A first authentication device (14), **characterized in that** the first authentication device is configured to:

- collect, based on a predetermined authentication policy, at least one context data element;
- constitute, based on the at least one collected context data element, a data packet;
- generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash; and
- send to a second authentication device the generated hash.

12. Device according to claim 11, wherein the first authentication device includes includes at least one element of a group including:
- a mobile phone;
- a Personal Computer;
- a vehicle;
- a desktop;
- a virtual reality device;
- an augment reality device;
- an Internet Of Things type device; and
- a computing device.

13. A second authentication device (16), **characterized in that** the second authentication device is configured to:
- receive a generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

14. Device according to claim 13, wherein the second authentication device includes at least one element of a group including:
- a secure element;
- a local server;
- a remote server;
- a mobile phone;
- a Personal Computer;
- a vehicle;

- a desktop;
- a virtual reality device;
- an augment reality device;
- an Internet Of Things type device;
- a computing device.

15. An authentication system (10), **characterized in that,** the system comprising a first authentication device (14) and at least one second authentication device (16), the first authentication device is configured to:

- collect, based on a predetermined authentication policy, at least one context data element;
- constitute, based on the at least one collected context data element, a data packet;
- generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- send to the second authentication device, the generated hash; and

in that the second authentication device is configured to:

- receive from the first device, the generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

Europäisches Patentamt
European Patent Office
Office européen des brevets

Bescheinigung	Certificate	Attestation
Die angehefteten Unterlagen stimmen mit der als ursprünglich eingereicht geltenden Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.	The attached documents are exact copies of the text in which the European patent application described on the following page is deemed to have been filed.	Les documents joints à la présente attestation sont conformes au texte, considéré comme initialement déposé, de la demande de brevet européen qui est spécifiée à la page suivante.

Patentanmeldung Nr.	**Patent application No.**	**Demande de brevet n°**
	17306977.4 / EP17306977	

The organisation code and number of your priority application, to be used for filing abroad under the Paris Convention, is EP17306977.

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le President de l'Office européen des brevets
p.o.

V. Joseph

Thales Exhibit 2001, Page 161 of 339
Okta v. Thales DIS France - IPR2026-00278

Anmeldung Nr:
Application no.: 17306977.4
Demande no :

Anmeldetag:
Date of filing: 29.12.17
Date de dépôt :

Anmelder / Applicant(s) / Demandeur(s):

GEMALTO SA
6, rue de la Verrerie
92190 Meudon/FR

Bezeichnung der Erfindung / Title of the invention / Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, oder falls die Anmeldung in einer Nicht-Amtssprache des EPA eingereicht wurde, siehe Beschreibung bezüglich ursprünglicher Bezeichnung.
If no title is shown, or if the application has been filed in a non-EPO language, please refer to the description for the original title.
Si aucun titre n'est indiqué, ou si la demande a été déposée dans une langue autre qu'une langue officielle de l'OEB, se référer à la description pour le titre original.)

AUTHENTICATION METHOD, DEVICE AND SYSTEM

In Anspruch genommene Priorität(en) / Priority(Priorities) claimed / Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen / State/Date/File no. / Pays/Date/Numéro de dépôt:

Am Anmeldetag benannte Vertragstaaten / Contracting States designated at date of filing / Etats contractants désignés lors du dépôt:

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Thales Exhibit 2001, Page 162 of 339
Okta v. Thales DIS France - IPR2026-00278

AUTHENTICATION METHOD, DEVICE AND SYSTEM

Field of the invention:

The present invention relates generally to an authentication method and an authentication device.

Furthermore, the invention pertains to an authentication system as well. The system includes at least two devices.

The present invention is notably applicable to a field in which a first device is e.g. a mobile (tele)phone or a Personal Computer (or PC) and a second device is e.g. a (local) Secure Element (or SE) or a remote server.

Within the present description, an SE is a smart object that includes a chip(s) that protect(s), as a tamper resistant component(s), access to stored data and that is intended to communicate data with a device(s), like e.g., an SE host device, and/or an SE user.

State of the art:

EP 2 924 603 A2 describes a user authentication technique based on a transmission, from a client to a server, of a captured video signal including a physical user characteristic(s) and a physical object(s)/element(s) in the user environment. The sever analyses the captured video signal to determine a value associated with each of the visual and audio elements, as environment characteristics. The server determines a total score for the captured video signal and compares the total score to a predetermined reference score. The server decides to authorize (or not) based on a comparison result.

However, such a known solution requires a big bandwidth, namely several Mb, for an upload of the captured video signal. Moreover, the uploaded captured video signal includes information that discloses the user environment and therefore private data.

There is a need of an alternative authentication solution while being more efficient and more secure than such an aforementioned known solution.

Summary of the invention:

The invention proposes a solution for satisfying the just herein above specified need by providing an authentication method.

According to the invention, the method comprises:

- collecting, based on a predetermined authentication policy, at least one context data element;

- constituting, based on the at least one collected context data element, a data packet;
- generating, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- sending the generated hash;
- generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and
- authenticating successfully or not based on the generated hash distance, as an authentication step.

The principle of the invention consists in capturing, at a client device side, (local) context (or environment) data element(s) depending on an authentication policy, building a corresponding data packet and determining with a predefined hash type algorithm and, as input, the data packet a corresponding hash. The client device sends the determined hash. Then, a hash distance between the determined hash and a predefined reference hash is determined. The thus determined hash distance is then used for authenticating (or not) the tested authentication context (under survey).

The authentication policy defines notably the number and/or the nature of the context data element(s) to be captured. The authentication policy may include data relating to the used (client) device, a user, object(s) or thing(s) to be locally present and detected. To capture the context data element(s), the invention does not impose any constraint. The client device may use a camera(s), a microphone(s) and/or one or several sensors that is(are) incorporated within or connected to the client device.

The invention (authentication) solution is, through the authentication policy, configurable and therefore adaptable to different (local) environment or context scenario(s).

Since the client device (or a cooperating device, such as an SE), where there is an environment to be authenticated, generates (or determines) a hash from a data packet resulting from captured environment or context data element(s), the hash is transmitted in a secure and protected manner.

A software component, such as a library, a hardware component and/or a device may carry out the hash distance generation step and the authentication step. The software component may be supported by the client device, a local device, such as an SE, cooperating with the client device, or a remote device, such as a remote server. The hardware component may be incorporated within or connected or coupled to the

client device, a local device, such as an SE, cooperating with the client device, or a remote device, such as a remote server.

It is noteworthy that the hash distance generation step provides a hash distance that allows to determine whether the generated hash is more or less close to a predefined reference hash. The hash distance allows inferring whether the corresponding captured context data element(s) is(are) or is(are) not successfully authenticated, i.e. sufficiently close to respective predetermined reference captured context data element(s).

The hash distance may be generated through a hash type comparison algorithm.

An authentication of the concerned (local) environment or context under survey is therefore carried out through such a hash distance that is specific to (or characterizes) the invention solution.

The hash distance allows the invention solution to be resilient to more or less small changes with respect to the predefined reference hash while still authenticating successfully the concerned (local) environment or context, i.e. the value of at least some captured (or collected) context data element(s) has changed slightly.

It is to be noted that the hash or digest, as a byte stream relating to original captured context data element(s), is a string of bits with a resulting length, from e.g. 32 bytes to e.g. a few kbytes. The resulting length may be (or not) variable according to the captured context data element(s).

The hash relates to the original (captured) context data element(s) and reduces the number of bits (or elements of information) to be transferred with respect to the original context data element(s).

Contrary to the aforementioned prior art solution, the invention solution does not need a large bandwidth to transmit data, including the hash, relating to the concerned environment or context, since the data relating to the concerned context includes only a few data (up to a few kbytes) to be transmitted.

Contrary to the aforementioned prior art solution, the invention solution is therefore efficient.

Moreover, the hash obfuscates the concerned original context data element(s), i.e. does not disclose any original context data element(s) in plain text.

Since no data relating to the privacy is transmitted in plain text, the invention is thus compliant with data privacy and therefore the Generation Data Protection Regulation (or GDPR).

Contrary to the aforementioned prior art solution, due to the use of a hash (and not the use of the concerned captured context data element(s) in plain text), the invention solution is secure.

The invention solution is an environment or context authentication solution that allows authenticating the concerned (local) environment or context under survey.

The invention solution is user convenient.

Advantageously, the predetermined hash type algorithm comprising a Locality Sensitive Hash (or LSH) type algorithm, the method further comprises, as the hash distance generation step and the authentication step, the following steps:

- generating, by using the locality sensitive hash type algorithm, a score, as a level of similarity between the generated hash and the predetermined reference hash;
- comparing the score to a predetermined threshold value;
- authenticating successfully only if the score is equal to or greater than the predetermined threshold value.

The LSH type algorithm, as a hash type algorithm, is advantageously used to generate a score, as a hash distance used for comparing the generated hash to the predefined reference hash.

The generated score is then checked with respect to a predefined threshold value, so as to authenticate (or not) the concerned context.

Thus, the invention solution may be, through the score, as the hash distance, more or less permissive with respect to the predefined reference hash that has to be approached by the generated hash from the collected context data element(s).

It is to be noted that the score is either the hash distance itself or the result of a computation derived from the (hash) distance depending on the used algorithm for comparing the generated hash.

According to an additional aspect, the invention is a first authentication device.

According to the invention, the first authentication device is configured to:

- collect, based on a predetermined authentication policy, at least one context data element;
- constitute, based on the at least one collected context data element, a data packet;

- generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash; and
- send to a second device the generated hash.

The first authentication device may be a mobile phone, a PC or any computing device.

According to an additional aspect, the invention is a second authentication device.

According to the invention, the second authentication device is configured to:

- receive a generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

The second authentication device may be a secure element, a remote server or any computing device.

According to still a further aspect, the invention is an authentication system.

According to the invention, the system comprising a first authentication device and at least one second authentication device, the first authentication device is configured to:

- collect, based on a predetermined authentication policy, at least one context data element;
- constitute, based on the at least one collected context data element, a data packet;
- generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- send to the second authentication device, the generated hash; and

the second authentication device is configured to:

- receive from the first device, the generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

Brief description of the drawings:

Additional features and advantages of the invention will be apparent from a detailed description of one preferred embodiment of the invention, given as an indicative and non-limitative example, in conjunction with the following drawings:

- Figure 1 illustrates a simplified diagram of an exemplary embodiment of a system comprising a mobile phone and a server, the phone being configured to collect, based on a predefined authentication policy, a data element(s) comprised within the phone context, constitute a corresponding data packet, generate a corresponding hash, and send to the server the hash, the server being configured to generate a hash distance between the hash and a predetermined reference hash and authenticate, based on to the hash distance, the concerned context, according to the invention; and
- Figure 2 represents an example of a flow of messages exchanged between the user, the phone and the server of the system of figure 1, so that the server receives a hash generated at the client side, generates a corresponding hash distance and authenticates (or not), thanks to the generated hash distance, the concerned context.

Detailed description:

Herein under is considered an exemplary embodiment in which the invention authentication method is implemented notably by a phone, as a client (computer) device and a standalone entity, i.e. without cooperating with another device, such as an SE, and a remote server.

According to another exemplary embodiment (not represented), the invention authentication method is implemented by a computer device, as a terminal, in cooperation with an SE embedded within or connected to the terminal. According to such an embodiment, the SE, as a local and second authentication device, is adapted to perform the functions that are carried out by the server and described herein below while enhancing the security of stored and/or processed data.

The SE may be an incorporated chip, as a chip soldered, possibly in a removable manner, like e.g., an embedded SE, an embedded Universal Integrated Circuit Card (or eUICC) or an integrated Universal Integrated Circuit Card (or iUICC), on a Printed Circuit Board (or PCB) of the terminal, or a chip that is coupled to the terminal and included within a Universal Serial Bus (or USB), a smart card or any other medium (that may have different form factors), as an SE host device. The chip may thus be fixed to or removable from its host device, like e.g., the mobile phone.

The invention does not impose any constraint as to a kind of the SE type.

Naturally, the herein below described embodiment is only for exemplifying purposes and is not considered to reduce the scope of the present invention.

Figure 1 shows schematically an (authentication) system 10 that includes a (mobile) phone 14 and a remote (web) server 16.

The system is arranged to authenticate (or not) a context 12 (or environment) under survey.

The context 12 includes e.g. a user 11, as the owner of the phone 14.

Additionally (or alternately), the context 12 includes e.g. a TeleVision (or TV) set 13, as a physical object or thing.

However, the invention (authentication) solution is also applicable when the context 12 includes one or several human beings (and/or animal(s)) and/or one or several (physical) things.

For the sake of simplicity, only one phone 14, as a first (authentication) device, and only one user 11 and one object, as context data elements, have been represented.

However, the server 16, as a second (authentication) device, manages a set of context accounts and respective reference (context) hashes that have been previously respectively registered while using the same invention authentication process.

Instead of being constituted by a phone, the first device may be constituted by e.g., a smart phone, a PC, a vehicle, a virtual reality device, an augmented reality device, an Internet Of Things type device, a set-top box, a tablet computer, a desktop computer, a laptop computer, a video player, an audio player, a media-player, a game console, a netbook, a Personal Digital Assistant (or PDA), and/or any other computer device. Such a list of first devices is given as mere examples for a first device that may be used without being exhaustive.

Instead of being constituted by a physical first device, a software component, such as a library, or a hardware component carries out the functions that are described infra and that are performed by the phone 14.

The phone 14 includes one or several Central Processing Unit(s) (or CPU), (micro)processor(s) and/or (micro)controller(s) (not represented), as data processing means, one or several memories (not represented), as data storing means, and one or several Input/Output (or I/O) interfaces (not represented).

The (or each) phone processor processes data originating from and/or intended to any internal component and data originating from and/or intended to any external device through one or several phone I/O interfaces.

The phone memories may include one or several EEPROMs (acronym for "Electrically Erasable Programmable Read-Only Memory"), one or several ROMs (acronym for "Read Only Memory"), one or several Flash memories and/or any other memories of different types, like e.g., one or several RAMs (acronym for "Random Access Memory").

The phone 14 supports one or several Operating Systems (or OS).

The phone 14 supports a client application that allows the phone 14 to send, after a context data element collection, a corresponding data packet constitution and a corresponding hash generation, to the server 16 information including the generated hash. The generated hash allows the server 16 to authenticate (or not) the concerned context 12.

A phone 14 memory (and/or a memory of another device connected or coupled to the phone 14) stores a Mobile Station International Subscriber Directory Number (or MSISDN), as the phone 14 number, and/or the like, as a phone 14 Identifiers (or ID), , an International Mobile Equipment Identity (or IMEI), an email address and/or other data that allow(s) uniquely identifying the phone 14, as the first device.

The phone I/O interface(s) may comprise (and/or be connected to) a display screen and a keyboard, as a phone Man Machine Interface (or MMI), so as to interact with the user 11.

The phone I/O interface(s) includes e.g., a camera 142, so as to capture or collect video or picture data that is included in the environment or context that is present in front of the camera 142.

The phone I/O interface(s) includes e.g., one or several sensors that allow each to collect data relating to the context of the phone 14.

The phone I/O interface(s) includes e.g., an antenna 144, allowing to transmit data, through a Radio-Frequency (or RF) link(s) 15, as a wireless link(s), via a possible (communication) network(s), to the server 16.

The RF may be fixed at several hundreds of MHz, e.g., around 850, 900, 1800, 1900 and/or 2100 MHz, as Long Range (or LR) type RF.

The RF link 15 between the phone 14 and the server 16 is at least mono-directional, namely at least an uplink, i.e. from the phone 14 to the server 16.

The channel may be related to an HyperText Transfer Protocol (or HTTP) (Secure) (registered trademark) type channel, an Over-The-Air (or OTA), an Over-The-Internet (or OTI) type channel or any other data communication channel.

The channel using the RF link 15 may be secure or unsecure.

The phone 14 is arranged to collect, based on a predetermined authentication policy, an image (or picture) (and/or a video signal) including image data relating to the user 11 face and image data relating to the TV 13, as data elements included in the context (relating to the phone 14).

To collect a context data element(s), the phone 14 may use a Machine Learning (or ML) engine to analyse a collected (or captured) image.

Each context data element is preferably a string of bits (or units of information) with an individual fixed length.

The authentication policy allows configuring the phone 14 to process data originating from a surrounding environment of the phone 14, so as to authenticate the concerned environment.

The authentication policy is preferably previously (prior to launching an authentication process) provided by the server 16 or another server (not represented) connected to the server 16. The authentication policy comprises a set of identified context data elements to be collected, so as to define context data element(s) to be collected.

As context data element(s), the context data element(s) may include, besides image data relating to the user face and image data relating to the TV 13, other data, such as a phone ID, a Service Set IDentifier (or SSID), an OS version ID, geolocation data (like e.g., Global Positioning System (or GPS) data), a user 11 heart rate (not represented) and/or other data. To collect a context data element(s), the phone 14 may get or retrieve data, such as a phone ID, stored in a memory included within the phone 14 or a device connected or coupled to the phone 14.

The authentication policy may also define how the concerned context data element(s) is transformed into a corresponding data packet, how the resulting data packet is possibly processed, such as grouped, ciphered, weighted and/or sorted, and/or how a corresponding hash has to be generated.

The authentication policy may comprise information allowing to group together at least certain collected context data elements with respect to the other collected context

data element(s). Thus, certain context data elements are to be grouped within one and the same group, such as data relating to the operation of the phone 14, like e.g., an SSID and/or an OS version ID, and/or data relating to the audio and/or visual environment.

When two or more collected context data elements are grouped, the concerned collected context data element group impacts the corresponding generated hash distance (or score) by increasing the hash distance (or score) variation, i.e. if at least one of the collected context data elements within a concerned group changes, then the resulting corresponding generated hash distance (or score) varies more than if all of the collected context data elements of the group were kept (individually) separated from each other.

The authentication policy may comprise data for requesting that a data packet that results from the context data element(s) (possibly grouped at least in part) has to be ciphered by using a key generated from submitted user authentication data (or one or several data items originating from one or several external sources, such as a thermometer) (instead of being ciphered, being processed by a keyed one way function (i.e. non reversible), such as HMAC type function). Such a data packet ciphering request may further specify to use a specific encryption key, a specific encryption key generation algorithm, a specific data encryption algorithm and/or a process to generate the concerned encryption key or algorithm. The encryption key may be generated by using user authentication data, such as a Personal Identity Number (or PIN), a One-Time Password (or OTP), a password and/or a biometric user feature(s), such as a one or several user fingerprints, a user iris, a user face and/or a user palm(s), and/or data provided by one or several external sources, such as an SE, as input to an (identified) key generation algorithm. The encryption key may be generated by using a Hash-based Message Authentication Code (or HMAC) key derivation function.

The authentication policy may comprise data for identifying a user authentication to be used for authenticating the user 11, when applicable, i.e. when the user authentication data is to be included in the context data element(s). For example, the user 11 has to authenticate by providing a PIN, an OTP, a password and/or a biometric user feature(s), such as a one or several user fingerprints, a user iris, a user face and/or a user palm(s).

The authentication policy may comprise one or several weights to be associated with a specific (identified) group(s) and/or a specific (identified) context data element(s), so as to give heavier importance to the concerned group(s) and/or context data element(s) with respect to the other collected group(s) and/or collected context data element(s) within a corresponding data packet.

The authentication policy may comprise data for requesting that, prior to generating a corresponding hash, the context data element(s) (possibly grouped at least in part) has to be sorted, according to a predetermined numerical order, such as an increasing or decreasing numerical order.

The authentication policy may comprise data for identifying a hash type algorithm to be used for generating a hash relating to the collected context data element(s).

The authentication policy may comprise data for identifying several hash type algorithms to be used for generating several hashes relating to the collected context data elements which may have separate natures of data elements. The corresponding hash distance (or score) to be generated is then averaged (or weighted) the hashes resulting from each hash type algorithms.

Optionally, the phone 14 is arranged, preferably according to the authentication policy, to group at least two collected context data elements within the collected context data elements within the data packet.

The phone 14 is adapted to constitute, based on the collected context data element(s), a (resulting) data packet by e.g. concatenating the collected context data element(s).

The data packet is a kind of passphrase comprising, as word(s), the collected context data element(s).

The data packet is a string of bits (or units of information) with a resulting length that may vary depending on the collected context data element length(s) between separate context authentication sessions. The data packet length corresponds to an addition of all of the individual length(s) relating to the collected context data element(s).

Optionally, the phone 14 is adapted, preferably according to the authentication policy, to cipher or encrypt the data packet. Each of the context data elements that are possibly grouped at least in part is thus ciphered by using a predetermined encryption key. The encryption key may have been generated by using a HMAC type derivation function.

Optionally, the phone is adapted to weigh, according to the authentication policy, one or several (identified) collected context data element(s) of the collected context data element(s) that may have been previously grouped within the data packet. Such a collected context data element weighing may depend on a predetermined hash type algorithm to be used for generating a hash. Such a collected context data element weighing allows favouring the concerned collected context data element(s) and/or the concerned context data group(s) with respect to the other context data elements comprised within the concerned data packet. To weigh the concerned context data element(s), the phone 14 may duplicate the concerned context data element(s).

Optionally, the phone is arranged preferably according to the authentication policy, to sort, according to a numerical order, such as an increasing or a decreasing numerical order, the collected context data element(s) within the data packet. Such a (collected) context data element sorting allows preserving, depending on the used hash type algorithm, a generation of a corresponding hash and therefore a corresponding hash distance, i.e. the hash to be generated does not change when the concerned context data element sorting order is kept.

According to an essential invention feature, the phone 14 is configured to generate a hash by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm.

The predetermined hash type algorithm may be one of the following algorithms: a Locality Sensitive Hash (or LSH) type algorithm, a fuzzy matching type algorithm, a Trend micro Locality Sensitive Hash (or TLSH) type algorithm, a nilsimsa type algorithm, an sdhash type algorithm, an ssdeep type algorithm, an approximate matching type algorithm, a near duplicate matching type algorithm and a similarity detection type algorithm.

Such a list of hash type algorithms is given without being exhaustive as mere examples for an hash type algorithm that may be used for generating a hash with, as input, a data packet.

The hash type algorithm may incorporate a weighting, within the collected context data element(s), of one or several context data elements and/or one or several context data element group(s).

The phone 14 is arranged to send to the server 16, as a second (authentication) device, the generated hash.

Such a generated hash, as a cipher and a kind of context signature, allows not to disclose any original (user) private data that has been locally collected and therefore preserve the data privacy.

The generated hash has a fixed length that is a few data (up to a few kbits).

Instead of being constituted by a (physical) server, the second device may be constituted by e.g., a smart phone, a PC, a vehicle, a virtual reality device, an augmented reality device, an Internet Of Things type device, a set-top box, a tablet computer, a desktop computer, a laptop computer, a video player, an audio player, a media-player, a game console, a netbook, a Personal Digital Assistant (or PDA), and/or any other computer device. Such a list of second devices is given as mere examples for a second device that may be used without being exhaustive.

Instead of being constituted by a physical second device, a software component, such as a library, or a hardware component carries out the functions that are described infra and that are performed by the server 16.

The server 16 is connected to the phone 14 over the link 15.

The server 16 is remote and accessible through possibly one, two or more communication networks, such as an Intranet network and/or an Internet network, that allow to define or form a corresponding communication channel.

The corresponding communication channel may be secure or unsecure.

According to an alternative embodiment (not represented), the server 16 is local. For example, the server 16 is embedded within a device, such as an SE that is connected or coupled to the PC 14.

The server 16 may be operated or managed by a Mobile Network Operator (or MNO), a Mobile Virtual Network Operator (or MVNO), a banking Operator, a wire communication network operator, a service Operator (or administrator) or on behalf of a service Operator, as a service provider.

The server 16 includes one or several CPU(s), (micro)processor(s) and/or (micro)controller(s) 162, as data processing means, one or several memories 164, as data storing means, and one or several I/O interfaces 166 that are internally together connected.

A (or the) server I/O interface 166 is used for communicating with external devices, such as the first device 14.

A (or the) server memory 164 stores preferably, besides an OS, an invention (server) authentication application accessible from the server 16 processor.

A (or the) server memory 164 stores or registers a database.

The database includes a set of e.g. first device accounts. The database relates to a set of e.g. first devices, as a fleet of first devices.

Each first device account may include one or several associated user identifiers, such as a user name.

The database includes preferably, in association with e.g. each (identified) first device account, a corresponding predetermined reference hash.

The predetermined reference hash has been previously (i.e. during an enrolment or registration phase and prior to any (context) authentication) registered while using the invention authentication process.

The database may associate, for each individual first device or the first device set, a registered predetermined hash type algorithm.

The predetermined hash type algorithm may be one of the following algorithms an LSH type algorithm, a fuzzy matching type algorithm, a TLSH type algorithm, a nilsimsa type algorithm, an sdhash type algorithm, an ssdeep type algorithm, an approximate matching type algorithm, a near duplicate matching type algorithm and a similarity detection type algorithm.

Such a list of hash type algorithms is given without being exhaustive as mere examples for an hash type algorithm that may be used for generating a hash distance with, as inputs, a generated hash (to be received from a client device) and a corresponding (registered) reference hash.

The database may associate, for each individual first device or the first device set, a registered predetermined threshold value.

The predetermined threshold value has been previously (i.e. prior to any (context) authentication) registered. The predetermined threshold value is configurable according to a level of risk that the concerned service provider may take.

The (or each) server processor processes data originating from and/or intended to any internal component and data originating from and/or intended to any external device through one or several server I/O interfaces.

The server 16 supports one or several OSs.

The server 16 supports a server application that allows the server 16, after a hash reception and a corresponding hash distance generation, to authenticate (or not), based on the hash distance, the concerned phone context.

The server 16 may be configured to generate and send an authentication policy to the first device, such as the phone 14, prior to any first device enrolment.

The server 16 is adapted to receive, from an (identified) client device, such as the phone 14, a generated hash.

The server 16 identifies, based on a received e.g. client device ID(s), a corresponding first device registered within the database accessible to the server 16.

Then, the server 16 retrieves a predetermined reference hash that is registered in association with the registered first device or a corresponding first device fleet.

According to an essential invention feature, the server 16 is configured to generate on-the-fly, i.e. when a first device launches a login (or connection) session with the server 16, a score, as a hash distance between the (received) generated hash and a (registered) predetermined reference hash.

To generate the score, the server 16 uses the (retrieved) predetermined hash type algorithm and the (retrieved) predetermined reference hash.

The server 16 is adapted to authenticate successfully or not, based on the generated hash distance, the concerned context 12.

More exactly, the server 16 is configured to fail to authenticate the context 12 if the generated hash distance is less than the (retrieved) predetermined threshold value.

The server 16 is configured to succeed in authenticating the context 12 if the generated hash distance is equal to or greater than the (retrieved) predetermined threshold value.

The server 16 may be adapted to store, preferably in a secure and persistent manner, the (received) generated hash, each time the authentication is successful. Such a generated hash storage when the authentication is successful allows to trace the success authentication history or evolvement.

Alternately (or additionally), each time the authentication is successful, the server 16 is arranged to register, instead of the predetermined reference hash, the (received) generated hash, as an updated reference hash to be used for a next authentication. The authentication process taking into account the last generated hash, as the updated

reference hash for a new (context) authentication, lets evolve the corresponding reference hash with the time at each authentication success.

Figure 2 depicts an example of a message flow 20 that involves the phone 14 and the server 16, so that the server 16 authenticates the context 12 based on a hash distance between a (received) generated hash and a (registered) predetermined reference hash.

It is assumed that the authentication policy has been provided during a personalization phase to the phone 14. The authentication policy requests to collect an image relating to the user 11 face, an image relating to the TV 13 and a phone ID, as three context data elements to be detected, so as to authenticate the user 11.

It is further assumed that the server 16 has previously registered (not represented) a user 11 ID in association with the phone 14 number, as a phone ID, a predetermined reference hash corresponding to the user 11 face image, the TV 13 image and the phone ID, as corresponding context data elements, a predetermined threshold value, such as e.g. 75%, and a predetermined hash type algorithm to be used for generating a hash distance.

It is assumed that the predetermined hash type algorithm to be used for generating a hash and a corresponding hash distance is e.g. a LSH type algorithm.

The use of an LSH type algorithm allows generating similar hashes, i.e. a hash distance or score that is good, i.e. the score is equal or greater than the predefined threshold value, when there is a slight change between the hash relating to the current context under survey and the reference hash relating to a corresponding reference context.

The phone 14 thus constitutes a reference first (communication) device to be locally present within the user 11 context 12, so as to authenticate, through the context 12, the user 11.

It is further assumed that the phone 14 accesses the phone 14 ID and an image signal captured by the phone camera 142.

An execution of the client application supported by the phone 14 is automatically launched (i.e. without any involvement of the user 11).

Alternately, the user 11 launches the client application while using an MMI that is included in or connected to the phone 14.

The phone 14 gets, through the phone camera 142, an image signal 22 relating to all the physical human(s) (and/or animal(s)) and/or thing(s) that are present in front of the phone 14.

In the present scenario, the image signal includes e.g. the user 11 face image and the TV 13 image.

The phone 14 retrieves (not represented) from a phone memory the MSISDN of the phone 14, as the phone 14 ID.

Instead of collecting the phone 14 ID from a phone memory, the phone 14 collects from a locally connected device, such as an SE that has preferably authenticate a user e.g. through a PIN comparison to a reference PIN that is stored in an SE memory, the phone 14 ID 23.

The phone 14 collects 24 the user 11 face image and the TV 13 image while extracting from the image signal 22 the user 11 face image and the TV 13 image and the phone 14 ID, as three context data elements required by the authentication policy.

The phone 14 may group 26, based on the authentication policy, at least two context data elements, e.g., the user 11 face image and the TV 13 image, as one and the same context data element group, within the collected data elements.

The phone 14 constitutes 28, based on the collected context data elements, a data packet by e.g. concatenating the collected context data elements

Optionally, the phone 14 enciphers 210, based on the authentication policy, the (resulting) data packet, so as to improve the security aspect. The data packet that is thus enciphered while using a key depending on e.g. user authentication impacts on the corresponding hash distance (or score). If the user is not successfully authenticated (at the client side), then the corresponding resulting hash is remote from a predetermined reference hash leading to a “bad” hash distance (or score) and therefore a failure of context authentication (even if the other collected context data element(s) is(are) right with respect to a collected reference context data element(s) that produces the corresponding predetermined reference hash).

The phone 14 may weigh 212, based on the authentication policy (or the used predetermined hash type algorithm), more or less heavy, one or several collected context data elements and/or one or several groups of collected context data elements with respect to the other collected context data elements within the data packet.

Optionally, the phone 14 sorts 214, according to a numerical order, such as a decreasing or an increasing order, the collected context data elements that are possibly grouped at least in part, possibly enciphered and/or possibly weighted, within the data packet.

Then, the phone 14 generates 216, by using e.g. a nilsimsa algorithm and the data packet, as input to the nilsimsa algorithm, a hash.

The phone 14 sends, through e.g., a Short Message Service (or SMS), Multimedia Messaging Service (or MMS), Transmission Control Protocol/Internet Protocol (or TCP/IP), or HTTP(s) type channel, to an (identified) server 16 a message 218 that includes the phone ID and the generated hash.

Once the server 16 has received the message, the server 16 identifies (not represented), based on the phone ID, the concerned user 11 account and thus the associated predetermined reference hash and the associated predetermined hash type algorithm to be used for generating a hash distance.

Then, the server 16 generates a hash distance between the (received) generated hash and the predetermined reference hash.

To generate the hash distance, the server 16 gets the reference hash and generates 220 a score by using e.g. the nilsimsa algorithm and the received generated hash and the predetermined reference hash, as the two inputs to the nilsimsa algorithm. The score is considered as a level of similarity between the received generated hash and the predetermined reference hash. For instance with the nilsimsa algorithm, the score is “0” (zero) when there is no similarity i.e.0% of similarity, is “96” when there is 75% of similarity and is “128” when there is a full similarity, i.e. 100% of similarity.

Once the server 16 has generated the hash distance, the server 16 verifies 222 whether the authentication is or is not successful based on the generated hash distance. To do such an authentication verification, the server 16 compares 222 the generated score with respect to the predetermined threshold value.

If the generated score is less than the predetermined threshold value, then the server 16 fails 223 to authenticate, through the user context 12, the user 11 and denies user access to the service(s) managed by or through the server 16.

Otherwise, i.e. if the generated score is equal to or greater than the predetermined threshold value, then the server 16 succeeds 224 in authenticating, through the user

context 12, the user 11 and grants user access to a service(s) managed by or through the server 16.

Optionally, if the generated score is equal to or greater than the predetermined threshold value, the server 16 registers 226 the received generated hash by either further enriching (or adding to) a database relating to the reference hashes in case of authentication success or substituting the received generated hash to the registered predetermined reference hash. Thus, in this latter case, the authentication process is continuously adaptive along the way the authentication context is evolving.

Optionally, the server 16 sends (not represented) to the phone 14, through the same channel or an out-of-band channel than the one used for the submission of the generated hash, a message that includes a request to present or display the authentication result. Then, the phone 14 presents or displays the authentication result (not represented), such as “authentication failure” or “authentication success”.

For the user, the invention solution is simple, easy, quick and practical since the user does not need to be involved. As a matter of fact, the user has just to present her or his face and the TV in front of the camera. The user does not need to enter any data, like e.g., an OTP, a number or a text on the first device, so as to let a first part collect the required context data elements and issue a corresponding hash to be verified by a second part, as its addressee, in order to be authenticated.

The invention solution allows carrying out a secure and efficient context authentication based on a hash distance that allows keeping flexibility.

The invention solution allows adapting to more or less small authentication context data element change(s), according to a level of risk to be adopted.

The invention solution does not include any oracle on the client (device) since it has no means for validating or verifying the generated hash. As a matter of fact, only the server is able to verify the generated hash.

The invention solution prevents thus from a client side brute-force attack of user authentication.

The embodiment that has just been described is not intended to limit the scope of the concerned invention. Other embodiments may be given. As another embodiment, instead of using an LR RF technology channel to transmit information to the second device, the first device uses a Short Range (or SR) RF technology(ies), like e.g., a Wi-

Fi, Bluetooth, a Near Field Communication or a Bluetooth Low Energy type technology(ies).

CLAIMS

1. An authentication method (20) comprising:

- collecting (24), based on a predetermined authentication policy, at least one context data element;
- constituting (28), based on the at least one collected context data element, a data packet;
- generating (216), by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- sending the generated hash;
- generating (220), as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and
- authenticating (224) successfully or not (223) based on the generated hash distance, as an authentication step.

2. Method according to claim 1, wherein, the predetermined hash type algorithm comprising a locality sensitive hash type algorithm, the method further comprises, as the hash distance generation step and the authentication step, the following steps:

- generating, by using the locality sensitive hash type algorithm, a score, as a level of similarity between the generated hash and the predetermined reference hash;
- comparing the score to a predetermined threshold value;
- authenticating successfully only if the score is equal to or greater than the predetermined threshold value.

3. Method according to claim 1 or 2, wherein, prior to generating the hash, the method further comprises sorting, according to a numerical order, the at least one collected context data element within the data packet.

4. Method according to any previous claim, wherein, prior to generating the hash, the method further comprises weighting, according to the authentication policy, at least one of the at least one context data element.

5. Method according to any previous claim, wherein, prior to constituting the data packet, the method further comprises grouping, according to the authentication policy,

together at least two context data elements comprised within the at least one context data element, to constitute at least one corresponding context data group.

6. Method according to any previous claim, wherein, prior to generating the hash, the method further comprises ciphering, according to the authentication policy, the data packet.

7. Method according to claim 6, wherein a key used for the data packet ciphering includes a key generated by using a hash-based message authentication code key type derivation function.

8. Method according to any previous claim, wherein the hash type algorithm includes at least one element of a group including:
- a locality sensitive hash type algorithm;
- a Trend micro Locality Sensitive Hash type algorithm;
- a nilsimsa type algorithm;
- an sdhash type algorithm;
- an ssdeep type algorithm; and
- a fuzzy matching type algorithm;
- an approximate matching type algorithm;
- a near duplicate matching type algorithm; and
- a similarity detection type algorithm.

9. Method according to any previous claim, wherein, each time the authentication is successful, the method further comprises storing the generated hash.

10. Method according to any previous claim, wherein, each time the authentication is successful, the method further comprises registering, instead of the predetermined reference hash, the generated hash, as an updated reference hash to be used for a next authentication.

11. A first authentication device (14), **characterized in that** the first authentication device is configured to:

- collect, based on a predetermined authentication policy, at least one context data element;
- constitute, based on the at least one collected context data element, a data packet;
- generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash; and
- send to a second authentication device the generated hash.

12. Device according to claim 11, wherein the first authentication device includes includes at least one element of a group including:
- a mobile phone;
- a Personal Computer;
- a vehicle;
- a desktop;
- a virtual reality device;
- an augment reality device;
- an Internet Of Things type device; and
- a computing device.

13. A second authentication device (16), **characterized in that** the second authentication device is configured to:
- receive a generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

14. Device according to claim 13, wherein the second authentication device includes at least one element of a group including:
- a secure element;
- a local server;
- a remote server;
- a mobile phone;
- a Personal Computer;
- a vehicle;

- a desktop;
- a virtual reality device;
- an augment reality device;
- an Internet Of Things type device;
- a computing device.

15. An authentication system (10), **characterized in that,** the system comprising a first authentication device (14) and at least one second authentication device (16), the first authentication device is configured to:

- collect, based on a predetermined authentication policy, at least one context data element;
- constitute, based on the at least one collected context data element, a data packet;
- generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- send to the second authentication device, the generated hash; and

in that the second authentication device is configured to:

- receive from the first device, the generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

AUTHENTICATION METHOD, DEVICE AND SYSTEM

ABSTRACT

The invention relates to an authentication method. The method comprises:

- collecting 24, based on a predetermined authentication policy, at least one context data element;
- constituting 28, based on the at least one collected context data element, a data packet;
- generating 216, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- sending the generated hash;
- generating 220, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and
- authenticating 224 successfully or not 223 based on the generated hash distance, as an authentication step.

The invention also relates to corresponding device and system.

Figure 2

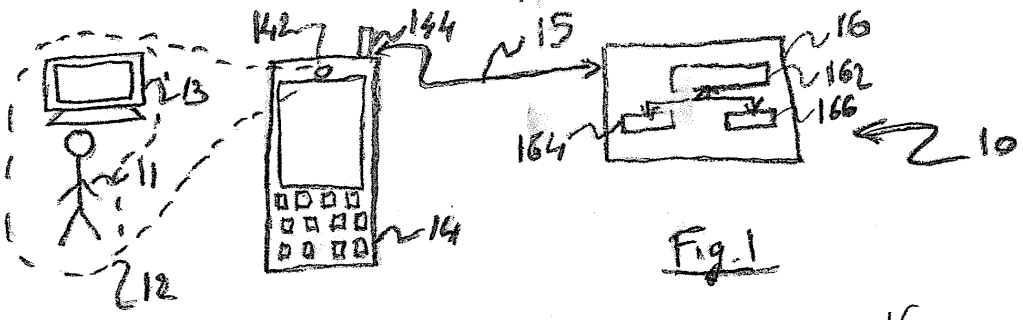

142
144
15
16
162
166
164
10
13
11
14
12

Fig. 1

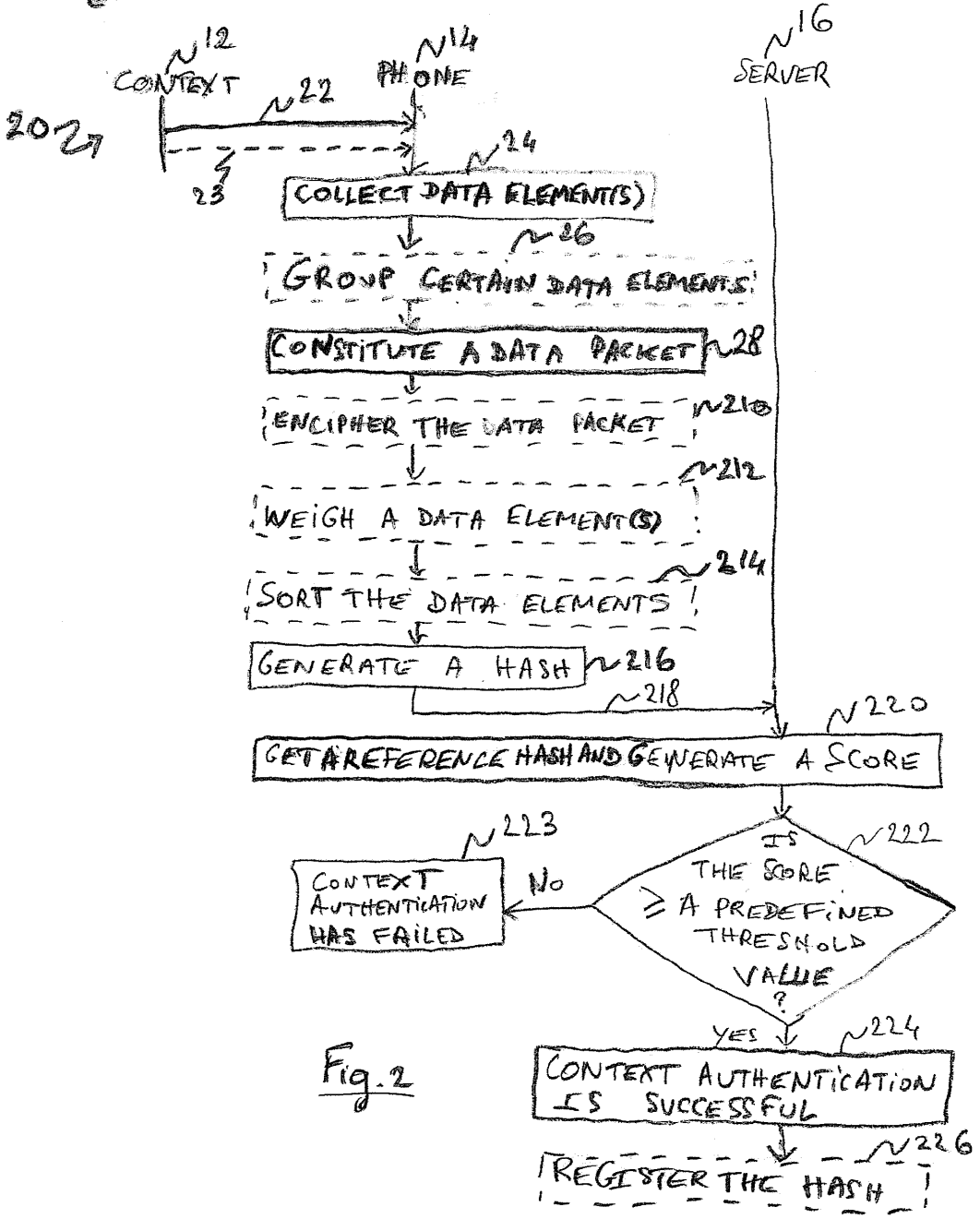

12
CONTEXT
14
PHONE
16
SERVER
20
22
23
24
COLLECT DATA ELEMENT(S)
26
GROUP CERTAIN DATA ELEMENTS
CONSTITUTE A DATA PACKET
28
ENCIPHER THE DATA PACKET
210
WEIGH A DATA ELEMENT(S)
212
SORT THE DATA ELEMENTS
214
GENERATE A HASH
216
218
GET A REFERENCE HASH AND GENERATE A SCORE
220
IS THE SCORE ≥ A PREDEFINED THRESHOLD VALUE ?
222
No
CONTEXT AUTHENTICATION HAS FAILED
223
YES
224
CONTEXT AUTHENTICATION IS SUCCESSFUL
226
REGISTER THE HASH

Fig. 2

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

DOCUMENT MADE AVAILABLE UNDER THE PATENT COOPERATION TREATY (PCT)

International application number:		**PCT/EP2018/081759**
International filing date:		**19 November 2018 (19.11.2018)**
Document type:		**Certified copy of priority document**
Document details:	Country/Office:	**EP**
	Number:	**17306977.4**
	Filing date:	**29 December 2017 (29.12.2017)**
Date of receipt at the International Bureau:		**28 November 2018 (28.11.2018)**

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-*bis*)

34, chemin des Colombettes
1211 Geneva 20, Switzerland
www.wipo.int

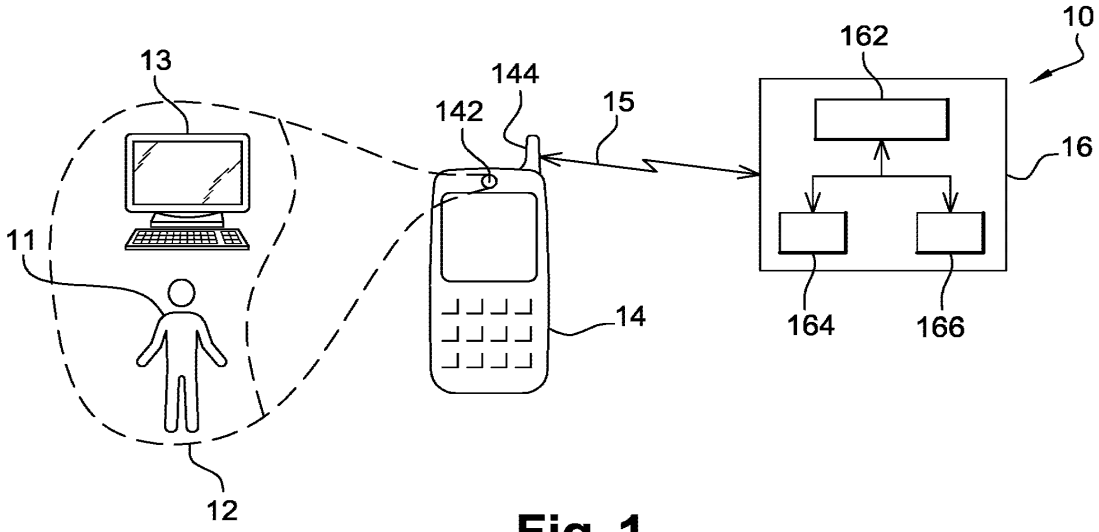


Fig. 1

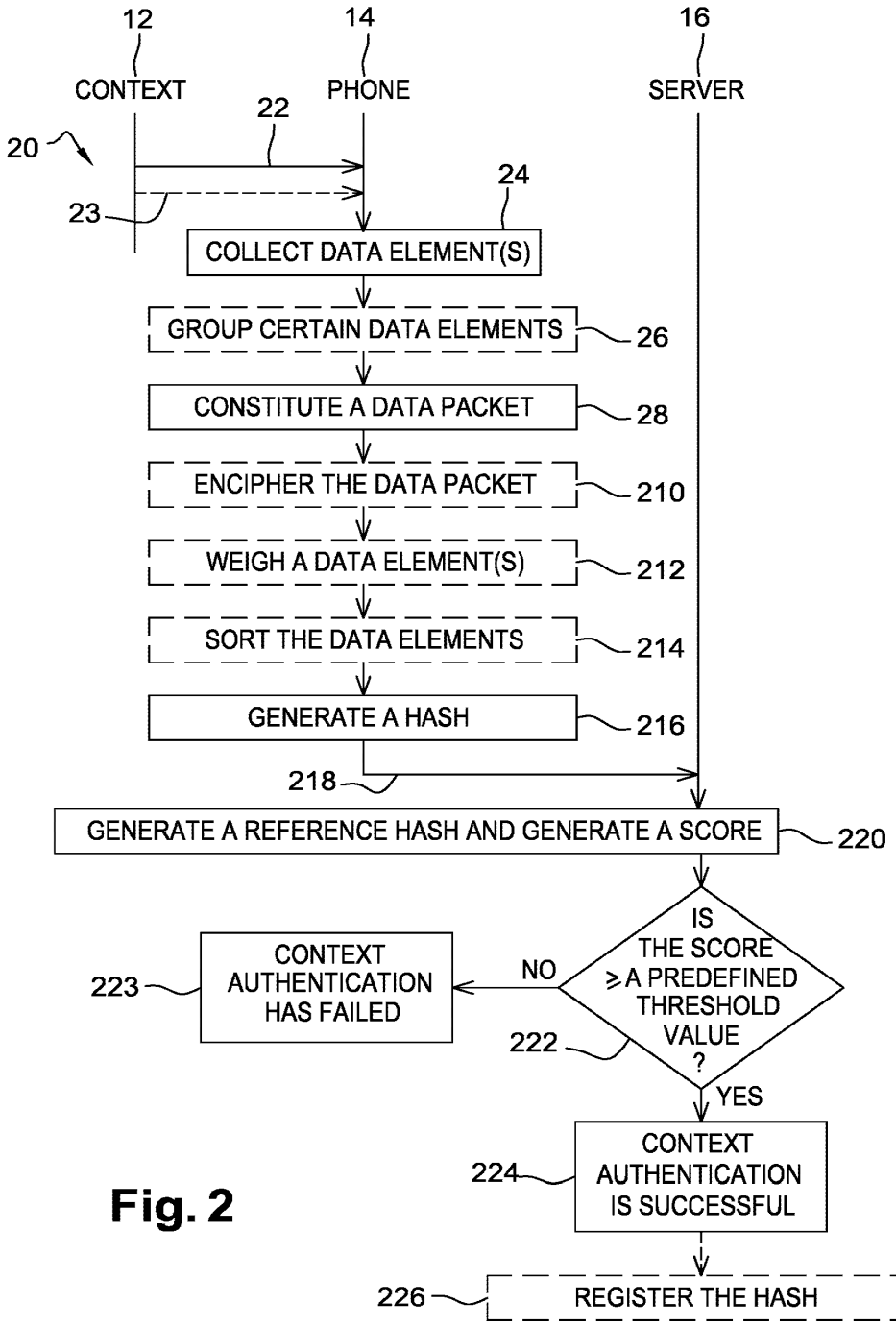

12
CONTEXT
14
PHONE
16
SERVER
20
22
23
24
COLLECT DATA ELEMENT(S)
GROUP CERTAIN DATA ELEMENTS
26
CONSTITUTE A DATA PACKET
28
ENCIPHER THE DATA PACKET
210
WEIGH A DATA ELEMENT(S)
212
SORT THE DATA ELEMENTS
214
GENERATE A HASH
216
218
GENERATE A REFERENCE HASH AND GENERATE A SCORE
220
IS THE SCORE ≥ A PREDEFINED THRESHOLD VALUE ?
222
NO
223
CONTEXT AUTHENTICATION HAS FAILED
YES
224
CONTEXT AUTHENTICATION IS SUCCESSFUL
226
REGISTER THE HASH

Fig. 2

AUTHENTICATION METHOD, DEVICE AND SYSTEM

Field of the invention:

The present invention relates generally to an authentication method and an authentication device.

Furthermore, the invention pertains to an authentication system as well. The system includes at least two devices.

The present invention is notably applicable to a field in which a first device is e.g. a mobile (tele)phone or a Personal Computer (or PC) and a second device is e.g. a (local) Secure Element (or SE) or a remote server.

Within the present description, an SE is a smart object that includes a chip(s) that protect(s), as a tamper resistant component(s), access to stored data and that is intended to communicate data with a device(s), like e.g., an SE host device, and/or an SE user.

State of the art:

EP 2 924 603 A2 describes a user authentication technique based on a transmission, from a client to a server, of a captured video signal including a physical user characteristic(s) and a physical object(s)/element(s) in the user environment. The sever analyses the captured video signal to determine a value associated with each of the visual and audio elements, as environment characteristics. The server determines a total score for the captured video signal and compares the total score to a predetermined reference score. The server decides to authorize (or not) based on a comparison result.

However, such a known solution requires a big bandwidth, namely several Mb, for an upload of the captured video signal. Moreover, the uploaded captured video signal includes information that discloses the user environment and therefore private data.

There is a need of an alternative authentication solution while being more efficient and more secure than such an aforementioned known solution.

Summary of the invention:

The invention proposes a solution for satisfying the just herein above specified need by providing an authentication method.

According to the invention, the method comprises:

- collecting, based on a predetermined authentication policy, at least one context data element;

- constituting, based on the at least one collected context data element, a data packet;
- generating, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- sending the generated hash;
- generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and
- authenticating successfully or not based on the generated hash distance, as an authentication step.

The principle of the invention consists in capturing, at a client device side, (local) context (or environment) data element(s) depending on an authentication policy, building a corresponding data packet and determining with a predefined hash type algorithm and, as input, the data packet a corresponding hash. The client device sends the determined hash. Then, a hash distance between the determined hash and a predefined reference hash is determined. The thus determined hash distance is then used for authenticating (or not) the tested authentication context (under survey).

The authentication policy defines notably the number and/or the nature of the context data element(s) to be captured. The authentication policy may include data relating to the used (client) device, a user, object(s) or thing(s) to be locally present and detected. To capture the context data element(s), the invention does not impose any constraint. The client device may use a camera(s), a microphone(s) and/or one or several sensors that is(are) incorporated within or connected to the client device.

The invention (authentication) solution is, through the authentication policy, configurable and therefore adaptable to different (local) environment or context scenario(s).

Since the client device (or a cooperating device, such as an SE), where there is an environment to be authenticated, generates (or determines) a hash from a data packet resulting from captured environment or context data element(s), the hash is transmitted in a secure and protected manner.

A software component, such as a library, a hardware component and/or a device may carry out the hash distance generation step and the authentication step. The software component may be supported by the client device, a local device, such as an SE, cooperating with the client device, or a remote device, such as a remote server. The hardware component may be incorporated within or connected or coupled to the

client device, a local device, such as an SE, cooperating with the client device, or a remote device, such as a remote server.

It is noteworthy that the hash distance generation step provides a hash distance that allows to determine whether the generated hash is more or less close to a predefined reference hash. The hash distance allows inferring whether the corresponding captured context data element(s) is(are) or is(are) not successfully authenticated, i.e. sufficiently close to respective predetermined reference captured context data element(s).

The hash distance may be generated through a hash type comparison algorithm.

An authentication of the concerned (local) environment or context under survey is therefore carried out through such a hash distance that is specific to (or characterizes) the invention solution.

The hash distance allows the invention solution to be resilient to more or less small changes with respect to the predefined reference hash while still authenticating successfully the concerned (local) environment or context, i.e. the value of at least some captured (or collected) context data element(s) has changed slightly.

It is to be noted that the hash or digest, as a byte stream relating to original captured context data element(s), is a string of bits with a resulting length, from e.g. 32 bytes to e.g. a few kbytes. The resulting length may be (or not) variable according to the captured context data element(s).

The hash relates to the original (captured) context data element(s) and reduces the number of bits (or elements of information) to be transferred with respect to the original context data element(s).

Contrary to the aforementioned prior art solution, the invention solution does not need a large bandwidth to transmit data, including the hash, relating to the concerned environment or context, since the data relating to the concerned context includes only a few data (up to a few kbytes) to be transmitted.

Contrary to the aforementioned prior art solution, the invention solution is therefore efficient.

Moreover, the hash obfuscates the concerned original context data element(s), i.e. does not disclose any original context data element(s) in plain text.

Since no data relating to the privacy is transmitted in plain text, the invention is thus compliant with data privacy and therefore the Generation Data Protection Regulation (or GDPR).

Contrary to the aforementioned prior art solution, due to the use of a hash (and not the use of the concerned captured context data element(s) in plain text), the invention solution is secure.

The invention solution is an environment or context authentication solution that allows authenticating the concerned (local) environment or context under survey.

The invention solution is user convenient.

Advantageously, the predetermined hash type algorithm comprising a Locality Sensitive Hash (or LSH) type algorithm, the method further comprises, as the hash distance generation step and the authentication step, the following steps:

- generating, by using the locality sensitive hash type algorithm, a score, as a level of similarity between the generated hash and the predetermined reference hash;
- comparing the score to a predetermined threshold value;
- authenticating successfully only if the score is equal to or greater than the predetermined threshold value.

The LSH type algorithm, as a hash type algorithm, is advantageously used to generate a score, as a hash distance used for comparing the generated hash to the predefined reference hash.

The generated score is then checked with respect to a predefined threshold value, so as to authenticate (or not) the concerned context.

Thus, the invention solution may be, through the score, as the hash distance, more or less permissive with respect to the predefined reference hash that has to be approached by the generated hash from the collected context data element(s).

It is to be noted that the score is either the hash distance itself or the result of a computation derived from the (hash) distance depending on the used algorithm for comparing the generated hash.

According to an additional aspect, the invention is a first authentication device.

According to the invention, the first authentication device is configured to:

- collect, based on a predetermined authentication policy, at least one context data element;
- constitute, based on the at least one collected context data element, a data packet;

- generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash; and
- send to a second device the generated hash.

The first authentication device may be a mobile phone, a PC or any computing device.

According to an additional aspect, the invention is a second authentication device.

According to the invention, the second authentication device is configured to:

- receive a generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

The second authentication device may be a secure element, a remote server or any computing device.

According to still a further aspect, the invention is an authentication system.

According to the invention, the system comprising a first authentication device and at least one second authentication device, the first authentication device is configured to:

- collect, based on a predetermined authentication policy, at least one context data element;
- constitute, based on the at least one collected context data element, a data packet;
- generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- send to the second authentication device, the generated hash; and

the second authentication device is configured to:

- receive from the first device, the generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

Brief description of the drawings:

Additional features and advantages of the invention will be apparent from a detailed description of one preferred embodiment of the invention, given as an indicative and non-limitative example, in conjunction with the following drawings:

- Figure 1 illustrates a simplified diagram of an exemplary embodiment of a system comprising a mobile phone and a server, the phone being configured to collect, based on a predefined authentication policy, a data element(s) comprised within the phone context, constitute a corresponding data packet, generate a corresponding hash, and send to the server the hash, the server being configured to generate a hash distance between the hash and a predetermined reference hash and authenticate, based on to the hash distance, the concerned context, according to the invention; and
- Figure 2 represents an example of a flow of messages exchanged between the user, the phone and the server of the system of figure 1, so that the server receives a hash generated at the client side, generates a corresponding hash distance and authenticates (or not), thanks to the generated hash distance, the concerned context.

Detailed description:

Herein under is considered an exemplary embodiment in which the invention authentication method is implemented notably by a phone, as a client (computer) device and a standalone entity, i.e. without cooperating with another device, such as an SE, and a remote server.

According to another exemplary embodiment (not represented), the invention authentication method is implemented by a computer device, as a terminal, in cooperation with an SE embedded within or connected to the terminal. According to such an embodiment, the SE, as a local and second authentication device, is adapted to perform the functions that are carried out by the server and described herein below while enhancing the security of stored and/or processed data.

The SE may be an incorporated chip, as a chip soldered, possibly in a removable manner, like e.g., an embedded SE, an embedded Universal Integrated Circuit Card (or eUICC) or an integrated Universal Integrated Circuit Card (or iUICC), on a Printed Circuit Board (or PCB) of the terminal, or a chip that is coupled to the terminal and included within a Universal Serial Bus (or USB), a smart card or any other medium (that may have different form factors), as an SE host device. The chip may thus be fixed to or removable from its host device, like e.g., the mobile phone.

The invention does not impose any constraint as to a kind of the SE type.

Naturally, the herein below described embodiment is only for exemplifying purposes and is not considered to reduce the scope of the present invention.

Figure 1 shows schematically an (authentication) system 10 that includes a (mobile) phone 14 and a remote (web) server 16.

The system is arranged to authenticate (or not) a context 12 (or environment) under survey.

The context 12 includes e.g. a user 11, as the owner of the phone 14.

Additionally (or alternately), the context 12 includes e.g. a TeleVision (or TV) set 13, as a physical object or thing.

However, the invention (authentication) solution is also applicable when the context 12 includes one or several human beings (and/or animal(s)) and/or one or several (physical) things.

For the sake of simplicity, only one phone 14, as a first (authentication) device, and only one user 11 and one object, as context data elements, have been represented.

However, the server 16, as a second (authentication) device, manages a set of context accounts and respective reference (context) hashes that have been previously respectively registered while using the same invention authentication process.

Instead of being constituted by a phone, the first device may be constituted by e.g., a smart phone, a PC, a vehicle, a virtual reality device, an augmented reality device, an Internet Of Things type device, a set-top box, a tablet computer, a desktop computer, a laptop computer, a video player, an audio player, a media-player, a game console, a netbook, a Personal Digital Assistant (or PDA), and/or any other computer device. Such a list of first devices is given as mere examples for a first device that may be used without being exhaustive.

Instead of being constituted by a physical first device, a software component, such as a library, or a hardware component carries out the functions that are described infra and that are performed by the phone 14.

The phone 14 includes one or several Central Processing Unit(s) (or CPU), (micro)processor(s) and/or (micro)controller(s) (not represented), as data processing means, one or several memories (not represented), as data storing means, and one or several Input/Output (or I/O) interfaces (not represented).

The (or each) phone processor processes data originating from and/or intended to any internal component and data originating from and/or intended to any external device through one or several phone I/O interfaces.

The phone memories may include one or several EEPROMs (acronym for "Electrically Erasable Programmable Read-Only Memory"), one or several ROMs (acronym for "Read Only Memory"), one or several Flash memories and/or any other memories of different types, like e.g., one or several RAMs (acronym for "Random Access Memory").

The phone 14 supports one or several Operating Systems (or OS).

The phone 14 supports a client application that allows the phone 14 to send, after a context data element collection, a corresponding data packet constitution and a corresponding hash generation, to the server 16 information including the generated hash. The generated hash allows the server 16 to authenticate (or not) the concerned context 12.

A phone 14 memory (and/or a memory of another device connected or coupled to the phone 14) stores a Mobile Station International Subscriber Directory Number (or MSISDN), as the phone 14 number, and/or the like, as a phone 14 Identifiers (or ID), , an International Mobile Equipment Identity (or IMEI), an email address and/or other data that allow(s) uniquely identifying the phone 14, as the first device.

The phone I/O interface(s) may comprise (and/or be connected to) a display screen and a keyboard, as a phone Man Machine Interface (or MMI), so as to interact with the user 11.

The phone I/O interface(s) includes e.g., a camera 142, so as to capture or collect video or picture data that is included in the environment or context that is present in front of the camera 142.

The phone I/O interface(s) includes e.g., one or several sensors that allow each to collect data relating to the context of the phone 14.

The phone I/O interface(s) includes e.g., an antenna 144, allowing to transmit data, through a Radio-Frequency (or RF) link(s) 15, as a wireless link(s), via a possible (communication) network(s), to the server 16.

The RF may be fixed at several hundreds of MHz, e.g., around 850, 900, 1800, 1900 and/or 2100 MHz, as Long Range (or LR) type RF.

The RF link 15 between the phone 14 and the server 16 is at least mono-directional, namely at least an uplink, i.e. from the phone 14 to the server 16.

The channel may be related to an HyperText Transfer Protocol (or HTTP) (Secure) (registered trademark) type channel, an Over-The-Air (or OTA), an Over-The-Internet (or OTI) type channel or any other data communication channel.

The channel using the RF link 15 may be secure or unsecure.

The phone 14 is arranged to collect, based on a predetermined authentication policy, an image (or picture) (and/or a video signal) including image data relating to the user 11 face and image data relating to the TV 13, as data elements included in the context (relating to the phone 14).

To collect a context data element(s), the phone 14 may use a Machine Learning (or ML) engine to analyse a collected (or captured) image.

Each context data element is preferably a string of bits (or units of information) with an individual fixed length.

The authentication policy allows configuring the phone 14 to process data originating from a surrounding environment of the phone 14, so as to authenticate the concerned environment.

The authentication policy is preferably previously (prior to launching an authentication process) provided by the server 16 or another server (not represented) connected to the server 16. The authentication policy comprises a set of identified context data elements to be collected, so as to define context data element(s) to be collected.

As context data element(s), the context data element(s) may include, besides image data relating to the user face and image data relating to the TV 13, other data, such as a phone ID, a Service Set IDentifier (or SSID), an OS version ID, geolocation data (like e.g., Global Positioning System (or GPS) data), a user 11 heart rate (not represented) and/or other data. To collect a context data element(s), the phone 14 may get or retrieve data, such as a phone ID, stored in a memory included within the phone 14 or a device connected or coupled to the phone 14.

The authentication policy may also define how the concerned context data element(s) is transformed into a corresponding data packet, how the resulting data packet is possibly processed, such as grouped, ciphered, weighted and/or sorted, and/or how a corresponding hash has to be generated.

The authentication policy may comprise information allowing to group together at least certain collected context data elements with respect to the other collected context

data element(s). Thus, certain context data elements are to be grouped within one and the same group, such as data relating to the operation of the phone 14, like e.g., an SSID and/or an OS version ID, and/or data relating to the audio and/or visual environment.

When two or more collected context data elements are grouped, the concerned collected context data element group impacts the corresponding generated hash distance (or score) by increasing the hash distance (or score) variation, i.e. if at least one of the collected context data elements within a concerned group changes, then the resulting corresponding generated hash distance (or score) varies more than if all of the collected context data elements of the group were kept (individually) separated from each other.

The authentication policy may comprise data for requesting that a data packet that results from the context data element(s) (possibly grouped at least in part) has to be ciphered by using a key generated from submitted user authentication data (or one or several data items originating from one or several external sources, such as a thermometer) (instead of being ciphered, being processed by a keyed one way function (i.e. non reversible), such as HMAC type function). Such a data packet ciphering request may further specify to use a specific encryption key, a specific encryption key generation algorithm, a specific data encryption algorithm and/or a process to generate the concerned encryption key or algorithm. The encryption key may be generated by using user authentication data, such as a Personal Identity Number (or PIN), a One-Time Password (or OTP), a password and/or a biometric user feature(s), such as a one or several user fingerprints, a user iris, a user face and/or a user palm(s), and/or data provided by one or several external sources, such as an SE, as input to an (identified) key generation algorithm. The encryption key may be generated by using a Hash-based Message Authentication Code (or HMAC) key derivation function.

The authentication policy may comprise data for identifying a user authentication to be used for authenticating the user 11, when applicable, i.e. when the user authentication data is to be included in the context data element(s). For example, the user 11 has to authenticate by providing a PIN, an OTP, a password and/or a biometric user feature(s), such as a one or several user fingerprints, a user iris, a user face and/or a user palm(s).

The authentication policy may comprise one or several weights to be associated with a specific (identified) group(s) and/or a specific (identified) context data element(s), so as to give heavier importance to the concerned group(s) and/or context data element(s) with respect to the other collected group(s) and/or collected context data element(s) within a corresponding data packet.

The authentication policy may comprise data for requesting that, prior to generating a corresponding hash, the context data element(s) (possibly grouped at least in part) has to be sorted, according to a predetermined numerical order, such as an increasing or decreasing numerical order.

The authentication policy may comprise data for identifying a hash type algorithm to be used for generating a hash relating to the collected context data element(s).

The authentication policy may comprise data for identifying several hash type algorithms to be used for generating several hashes relating to the collected context data elements which may have separate natures of data elements. The corresponding hash distance (or score) to be generated is then averaged (or weighted) the hashes resulting from each hash type algorithms.

Optionally, the phone 14 is arranged, preferably according to the authentication policy, to group at least two collected context data elements within the collected context data elements within the data packet.

The phone 14 is adapted to constitute, based on the collected context data element(s), a (resulting) data packet by e.g. concatenating the collected context data element(s).

The data packet is a kind of passphrase comprising, as word(s), the collected context data element(s).

The data packet is a string of bits (or units of information) with a resulting length that may vary depending on the collected context data element length(s) between separate context authentication sessions. The data packet length corresponds to an addition of all of the individual length(s) relating to the collected context data element(s).

Optionally, the phone 14 is adapted, preferably according to the authentication policy, to cipher or encrypt the data packet. Each of the context data elements that are possibly grouped at least in part is thus ciphered by using a predetermined encryption key. The encryption key may have been generated by using a HMAC type derivation function.

Optionally, the phone is adapted to weigh, according to the authentication policy, one or several (identified) collected context data element(s) of the collected context data element(s) that may have been previously grouped within the data packet. Such a collected context data element weighing may depend on a predetermined hash type algorithm to be used for generating a hash. Such a collected context data element weighing allows favouring the concerned collected context data element(s) and/or the concerned context data group(s) with respect to the other context data elements comprised within the concerned data packet. To weigh the concerned context data element(s), the phone 14 may duplicate the concerned context data element(s).

Optionally, the phone is arranged preferably according to the authentication policy, to sort, according to a numerical order, such as an increasing or a decreasing numerical order, the collected context data element(s) within the data packet. Such a (collected) context data element sorting allows preserving, depending on the used hash type algorithm, a generation of a corresponding hash and therefore a corresponding hash distance, i.e. the hash to be generated does not change when the concerned context data element sorting order is kept.

According to an essential invention feature, the phone 14 is configured to generate a hash by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm.

The predetermined hash type algorithm may be one of the following algorithms: a Locality Sensitive Hash (or LSH) type algorithm, a fuzzy matching type algorithm, a Trend micro Locality Sensitive Hash (or TLSH) type algorithm, a nilsimsa type algorithm, an sdhash type algorithm, an ssdeep type algorithm, an approximate matching type algorithm, a near duplicate matching type algorithm and a similarity detection type algorithm.

Such a list of hash type algorithms is given without being exhaustive as mere examples for an hash type algorithm that may be used for generating a hash with, as input, a data packet.

The hash type algorithm may incorporate a weighting, within the collected context data element(s), of one or several context data elements and/or one or several context data element group(s).

The phone 14 is arranged to send to the server 16, as a second (authentication) device, the generated hash.

Such a generated hash, as a cipher and a kind of context signature, allows not to disclose any original (user) private data that has been locally collected and therefore preserve the data privacy.

The generated hash has a fixed length that is a few data (up to a few kbits).

Instead of being constituted by a (physical) server, the second device may be constituted by e.g., a smart phone, a PC, a vehicle, a virtual reality device, an augmented reality device, an Internet Of Things type device, a set-top box, a tablet computer, a desktop computer, a laptop computer, a video player, an audio player, a media-player, a game console, a netbook, a Personal Digital Assistant (or PDA), and/or any other computer device. Such a list of second devices is given as mere examples for a second device that may be used without being exhaustive.

Instead of being constituted by a physical second device, a software component, such as a library, or a hardware component carries out the functions that are described infra and that are performed by the server 16.

The server 16 is connected to the phone 14 over the link 15.

The server 16 is remote and accessible through possibly one, two or more communication networks, such as an Intranet network and/or an Internet network, that allow to define or form a corresponding communication channel.

The corresponding communication channel may be secure or unsecure.

According to an alternative embodiment (not represented), the server 16 is local. For example, the server 16 is embedded within a device, such as an SE that is connected or coupled to the PC 14.

The server 16 may be operated or managed by a Mobile Network Operator (or MNO), a Mobile Virtual Network Operator (or MVNO), a banking Operator, a wire communication network operator, a service Operator (or administrator) or on behalf of a service Operator, as a service provider.

The server 16 includes one or several CPU(s), (micro)processor(s) and/or (micro)controller(s) 162, as data processing means, one or several memories 164, as data storing means, and one or several I/O interfaces 166 that are internally together connected.

A (or the) server I/O interface 166 is used for communicating with external devices, such as the first device 14.

A (or the) server memory 164 stores preferably, besides an OS, an invention (server) authentication application accessible from the server 16 processor.

A (or the) server memory 164 stores or registers a database.

The database includes a set of e.g. first device accounts. The database relates to a set of e.g. first devices, as a fleet of first devices.

Each first device account may include one or several associated user identifiers, such as a user name.

The database includes preferably, in association with e.g. each (identified) first device account, a corresponding predetermined reference hash.

The predetermined reference hash has been previously (i.e. during an enrolment or registration phase and prior to any (context) authentication) registered while using the invention authentication process.

The database may associate, for each individual first device or the first device set, a registered predetermined hash type algorithm.

The predetermined hash type algorithm may be one of the following algorithms an LSH type algorithm, a fuzzy matching type algorithm, a TLSH type algorithm, a nilsimsa type algorithm, an sdhash type algorithm, an ssdeep type algorithm, an approximate matching type algorithm, a near duplicate matching type algorithm and a similarity detection type algorithm.

Such a list of hash type algorithms is given without being exhaustive as mere examples for an hash type algorithm that may be used for generating a hash distance with, as inputs, a generated hash (to be received from a client device) and a corresponding (registered) reference hash.

The database may associate, for each individual first device or the first device set, a registered predetermined threshold value.

The predetermined threshold value has been previously (i.e. prior to any (context) authentication) registered. The predetermined threshold value is configurable according to a level of risk that the concerned service provider may take.

The (or each) server processor processes data originating from and/or intended to any internal component and data originating from and/or intended to any external device through one or several server I/O interfaces.

The server 16 supports one or several OSs.

The server 16 supports a server application that allows the server 16, after a hash reception and a corresponding hash distance generation, to authenticate (or not), based on the hash distance, the concerned phone context.

The server 16 may be configured to generate and send an authentication policy to the first device, such as the phone 14, prior to any first device enrolment.

The server 16 is adapted to receive, from an (identified) client device, such as the phone 14, a generated hash.

The server 16 identifies, based on a received e.g. client device ID(s), a corresponding first device registered within the database accessible to the server 16.

Then, the server 16 retrieves a predetermined reference hash that is registered in association with the registered first device or a corresponding first device fleet.

According to an essential invention feature, the server 16 is configured to generate on-the-fly, i.e. when a first device launches a login (or connection) session with the server 16, a score, as a hash distance between the (received) generated hash and a (registered) predetermined reference hash.

To generate the score, the server 16 uses the (retrieved) predetermined hash type algorithm and the (retrieved) predetermined reference hash.

The server 16 is adapted to authenticate successfully or not, based on the generated hash distance, the concerned context 12.

More exactly, the server 16 is configured to fail to authenticate the context 12 if the generated hash distance is less than the (retrieved) predetermined threshold value.

The server 16 is configured to succeed in authenticating the context 12 if the generated hash distance is equal to or greater than the (retrieved) predetermined threshold value.

The server 16 may be adapted to store, preferably in a secure and persistent manner, the (received) generated hash, each time the authentication is successful. Such a generated hash storage when the authentication is successful allows to trace the success authentication history or evolvement.

Alternately (or additionally), each time the authentication is successful, the server 16 is arranged to register, instead of the predetermined reference hash, the (received) generated hash, as an updated reference hash to be used for a next authentication. The authentication process taking into account the last generated hash, as the updated

reference hash for a new (context) authentication, lets evolve the corresponding reference hash with the time at each authentication success.

Figure 2 depicts an example of a message flow 20 that involves the phone 14 and the server 16, so that the server 16 authenticates the context 12 based on a hash distance between a (received) generated hash and a (registered) predetermined reference hash.

It is assumed that the authentication policy has been provided during a personalization phase to the phone 14. The authentication policy requests to collect an image relating to the user 11 face, an image relating to the TV 13 and a phone ID, as three context data elements to be detected, so as to authenticate the user 11.

It is further assumed that the server 16 has previously registered (not represented) a user 11 ID in association with the phone 14 number, as a phone ID, a predetermined reference hash corresponding to the user 11 face image, the TV 13 image and the phone ID, as corresponding context data elements, a predetermined threshold value, such as e.g. 75%, and a predetermined hash type algorithm to be used for generating a hash distance.

It is assumed that the predetermined hash type algorithm to be used for generating a hash and a corresponding hash distance is e.g. a LSH type algorithm.

The use of an LSH type algorithm allows generating similar hashes, i.e. a hash distance or score that is good, i.e. the score is equal or greater than the predefined threshold value, when there is a slight change between the hash relating to the current context under survey and the reference hash relating to a corresponding reference context.

The phone 14 thus constitutes a reference first (communication) device to be locally present within the user 11 context 12, so as to authenticate, through the context 12, the user 11.

It is further assumed that the phone 14 accesses the phone 14 ID and an image signal captured by the phone camera 142.

An execution of the client application supported by the phone 14 is automatically launched (i.e. without any involvement of the user 11).

Alternately, the user 11 launches the client application while using an MMI that is included in or connected to the phone 14.

The phone 14 gets, through the phone camera 142, an image signal 22 relating to all the physical human(s) (and/or animal(s)) and/or thing(s) that are present in front of the phone 14.

In the present scenario, the image signal includes e.g. the user 11 face image and the TV 13 image.

The phone 14 retrieves (not represented) from a phone memory the MSISDN of the phone 14, as the phone 14 ID.

Instead of collecting the phone 14 ID from a phone memory, the phone 14 collects from a locally connected device, such as an SE that has preferably authenticate a user e.g. through a PIN comparison to a reference PIN that is stored in an SE memory, the phone 14 ID 23.

The phone 14 collects 24 the user 11 face image and the TV 13 image while extracting from the image signal 22 the user 11 face image and the TV 13 image and the phone 14 ID, as three context data elements required by the authentication policy.

The phone 14 may group 26, based on the authentication policy, at least two context data elements, e.g., the user 11 face image and the TV 13 image, as one and the same context data element group, within the collected data elements.

The phone 14 constitutes 28, based on the collected context data elements, a data packet by e.g. concatenating the collected context data elements

Optionally, the phone 14 enciphers 210, based on the authentication policy, the (resulting) data packet, so as to improve the security aspect. The data packet that is thus enciphered while using a key depending on e.g. user authentication impacts on the corresponding hash distance (or score). If the user is not successfully authenticated (at the client side), then the corresponding resulting hash is remote from a predetermined reference hash leading to a "bad" hash distance (or score) and therefore a failure of context authentication (even if the other collected context data element(s) is(are) right with respect to a collected reference context data element(s) that produces the corresponding predetermined reference hash).

The phone 14 may weigh 212, based on the authentication policy (or the used predetermined hash type algorithm), more or less heavy, one or several collected context data elements and/or one or several groups of collected context data elements with respect to the other collected context data elements within the data packet.

Optionally, the phone 14 sorts 214, according to a numerical order, such as a decreasing or an increasing order, the collected context data elements that are possibly grouped at least in part, possibly enciphered and/or possibly weighted, within the data packet.

Then, the phone 14 generates 216, by using e.g. a nilsimsa algorithm and the data packet, as input to the nilsimsa algorithm, a hash.

The phone 14 sends, through e.g., a Short Message Service (or SMS), Multimedia Messaging Service (or MMS), Transmission Control Protocol/Internet Protocol (or TCP/IP), or HTTP(s) type channel, to an (identified) server 16 a message 218 that includes the phone ID and the generated hash.

Once the server 16 has received the message, the server 16 identifies (not represented), based on the phone ID, the concerned user 11 account and thus the associated predetermined reference hash and the associated predetermined hash type algorithm to be used for generating a hash distance.

Then, the server 16 generates a hash distance between the (received) generated hash and the predetermined reference hash.

To generate the hash distance, the server 16 gets the reference hash and generates 220 a score by using e.g. the nilsimsa algorithm and the received generated hash and the predetermined reference hash, as the two inputs to the nilsimsa algorithm. The score is considered as a level of similarity between the received generated hash and the predetermined reference hash. For instance with the nilsimsa algorithm, the score is “0” (zero) when there is no similarity i.e.0% of similarity, is “96” when there is 75% of similarity and is “128” when there is a full similarity, i.e. 100% of similarity.

Once the server 16 has generated the hash distance, the server 16 verifies 222 whether the authentication is or is not successful based on the generated hash distance. To do such an authentication verification, the server 16 compares 222 the generated score with respect to the predetermined threshold value.

If the generated score is less than the predetermined threshold value, then the server 16 fails 223 to authenticate, through the user context 12, the user 11 and denies user access to the service(s) managed by or through the server 16.

Otherwise, i.e. if the generated score is equal to or greater than the predetermined threshold value, then the server 16 succeeds 224 in authenticating, through the user

context 12, the user 11 and grants user access to a service(s) managed by or through the server 16.

Optionally, if the generated score is equal to or greater than the predetermined threshold value, the server 16 registers 226 the received generated hash by either further enriching (or adding to) a database relating to the reference hashes in case of authentication success or substituting the received generated hash to the registered predetermined reference hash. Thus, in this latter case, the authentication process is continuously adaptive along the way the authentication context is evolving.

Optionally, the server 16 sends (not represented) to the phone 14, through the same channel or an out-of-band channel than the one used for the submission of the generated hash, a message that includes a request to present or display the authentication result. Then, the phone 14 presents or displays the authentication result (not represented), such as “authentication failure” or “authentication success”.

For the user, the invention solution is simple, easy, quick and practical since the user does not need to be involved. As a matter of fact, the user has just to present her or his face and the TV in front of the camera. The user does not need to enter any data, like e.g., an OTP, a number or a text on the first device, so as to let a first part collect the required context data elements and issue a corresponding hash to be verified by a second part, as its addressee, in order to be authenticated.

The invention solution allows carrying out a secure and efficient context authentication based on a hash distance that allows keeping flexibility.

The invention solution allows adapting to more or less small authentication context data element change(s), according to a level of risk to be adopted.

The invention solution does not include any oracle on the client (device) since it has no means for validating or verifying the generated hash. As a matter of fact, only the server is able to verify the generated hash.

The invention solution prevents thus from a client side brute-force attack of user authentication.

The embodiment that has just been described is not intended to limit the scope of the concerned invention. Other embodiments may be given. As another embodiment, instead of using an LR RF technology channel to transmit information to the second device, the first device uses a Short Range (or SR) RF technology(ies), like e.g., a Wi-

Fi, Bluetooth, a Near Field Communication or a Bluetooth Low Energy type technology(ies).

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
04 July 2019 (04.07.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/129422 A1

(51) International Patent Classification:
G06F 21/32 (2013.01) *G06F 21/35* (2013.01)

(21) International Application Number:
PCT/EP2018/081759

(22) International Filing Date:
19 November 2018 (19.11.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
17306977.4 29 December 2017 (29.12.2017) EP

(71) Applicant: **GEMALTO SA** [FR/FR]; 6 Rue de la Verrerie, 92190 MEUDON (FR).

(72) Inventors: **DELHOSTE, Fabrice**; C/O GEMALTO SA, Service Brevets, 525 avenue du Pic de Bertagne, CS 12023, 13881 GEMENOS Cedex (FR). **PAILLART, Frédéric**; C/O GEMALTO SA, Service Brevets, 525 avenue du Pic de Bertagne, CS 12023, 13881 GEMENOS Cedex (FR). **PETIT, Sébastien**; C/O GEMALTO SA, Service Brevets, 525 avenue du Pic de Bertagne, CS 12023, 13881 GEMENOS Cedex (FR).

(74) Agent: **SCHEER, Luc**; 525 avenue du Pic de Bertagne CS 12023, 13881 Gemenos Cedex (FR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: AUTHENTICATION METHOD, DEVICE AND SYSTEM

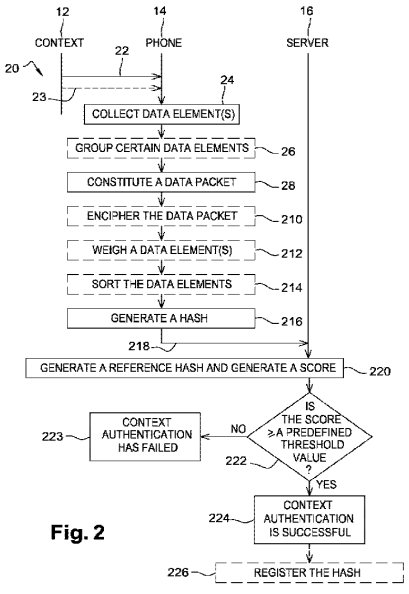


Fig. 2

(57) Abstract: The invention relates to an authentication method. The method comprises: - collecting (24), based on a predetermined authentication policy, at least one context data element; - constituting (28), based on the at least one collected context data element, a data packet; - generating (216), by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash; - sending the generated hash; - generating (220), as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and - authenticating (224) successfully or not (223) based on the generated hash distance, as an authentication step. The invention also relates to corresponding device and system.

[Continued on next page]

WO 2019/129422 A1

Published:
— *with international search report (Art. 21(3))*
— *with amended claims (Art. 19(1))*

Expéditeur : le BUREAU INTERNATIONAL

PCT

NOTIFICATION DE L'ENREGISTREMENT
D'UN CHANGEMENT

(règle 92*bis*.1 et instruction administrative 422 du PCT)

Destinataire :

SCHEER, Luc
525 avenue du Pic de Bertagne CS 12023
13881 Gemenos Cedex
FRANCE

Date d'expédition *(jour/mois/année)*
12 août 2019 (12.08.2019)

Référence du dossier du déposant ou du mandataire
GMT3707WO/DD

NOTIFICATION IMPORTANTE

Demande internationale n°
PCT/EP2018/081759

Date du dépôt international *(jour/mois/année)*
19 novembre 2018 (19.11.2018)

1. Les renseignements suivants étaient enregistrés en ce qui concerne :

☒ le déposant ☐ l'inventeur ☐ le mandataire ☐ le représentant commun

Nom et adresse
GEMALTO SA
6, rue de la Verrerie
92190 Meudon
FRANCE

Nationalité (nom de l'Etat) : FR
Domicile (nom de l'Etat) : FR
n° de téléphone :
n° de télécopieur :
Address électronique :

2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne :

☐ la personne ☐ le nom ☒ l'adresse ☐ la nationalité ☐ le domicile

Nom et adresse
THALES DIS FRANCE SA
6, rue de la Verrerie
92190 Meudon
FRANCE

Nationalité (nom de l'Etat) : FR
Domicile (nom de l'Etat) : FR
n° de téléphone :
n° de télécopieur :
Address électronique :
☐ Autorisation de recourir au courrier électronique

3. Observations complémentaires, le cas échéant :

4. Une copie de cette notification a été envoyée

☒ à l'office récepteur
☐ à l'administration chargée de la recherche internationale
☐ [à l'] [aux] administration(s) indiquée(s) pour la recherche supplémentaire
☐ à l'administration chargée de l'examen préliminaire international
☒ aux offices désignés concernés
☐ aux offices élus concernés
☐ autre destinataire :

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

Fonctionnaire autorisé
Nissen Diana
e-mail diana.nissen@wipo.int
n° de téléphone +4122 338 8054

Formulaire PCT/IB/306 (janvier 2009) 1/RRH5JE9KJ9F9M11

PCT REQUEST

Print Out (Original in Electronic Form)

0	**For receiving Office use only**	
0-1	International Application No.	**PCT/EP2018/081759**
0-2	International Filing Date	**19 NOV 2018 (19.11.2018)**
0-3	Name of receiving Office and "PCT International Application"	**RO/EP**

0-4	**Form PCT/RO/101 PCT Request**	
0-4-1	Prepared Using	PCT Online Filing Version 3.51.000.259e MT/FOP 20141031/0.20.5.20
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	European Patent Office (EPO) (RO/EP)
0-7	**Applicant's or agent's file reference**	GMT3707WO/DD
I	**Title of Invention**	AUTHENTICATION METHOD, DEVICE AND SYSTEM
II	**Applicant**	
II-1	This person is	Applicant only
II-2	Applicant for	All designated States
II-4	Name	GEMALTO SA
II-5	Address	6 Rue de la Verrerie 92190 MEUDON France
II-6	State of nationality	FR
II-7	State of residence	FR
III-1	**Applicant and/or inventor**	
III-1-1	This person is	Inventor only
III-1-3	Inventor for	All designated States
III-1-4	Name (LAST, First)	DELHOSTE, Fabrice
III-1-5	Address	C/O GEMALTO SA Service Brevets 525 avenue du Pic de Bertagne CS 12023 13881 GEMENOS Cedex France

PCT REQUEST

Print Out (Original in Electronic Form)

III-2	**Applicant and/or inventor**	
III-2-1	This person is	Inventor only
III-2-3	Inventor for	All designated States
III-2-4	Name (LAST, First)	PAILLART, Frédéric
III-2-5	Address	C/O GEMALTO SA Service Brevets 525 avenue du Pic de Bertagne CS 12023 13881 GEMENOS Cedex France
III-3	**Applicant and/or inventor**	
III-3-1	This person is	Inventor only
III-3-3	Inventor for	All designated States
III-3-4	Name (LAST, First)	PETIT, Sébastien
III-3-5	Address	C/O GEMALTO SA Service Brevets 525 avenue du Pic de Bertagne CS 12023 13881 GEMENOS Cedex France
IV-1	**Agent or common representative; or address for correspondence** The person identified below is hereby/ has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	Agent
IV-1-1	Name (LAST, First)	SCHEER, Luc
IV-1-2	Address	525 avenue du Pic de Bertagne CS 12023 13881 Gemenos Cedex France
IV-1-3	Telephone No.	+33 4 42 36 43 04
IV-1-4	Facsimile No.	+33 4 42 36 63 43
IV-1-5	e-mail	david.dages@gemalto.com
IV-1-5(a)	E-mail authorization The receiving Office, the International Searching Authority, the International Bureau and the International Preliminary Examining Authority are authorized to use this e-mail address, if the Office or Authority so wishes, to send notifications issued in respect of this international application:	exclusively in electronic form (no paper notifications will be sent)
V	**DESIGNATIONS**	
V-1	**The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the international filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents.**	

PCT REQUEST

Print Out (Original in Electronic Form)

VI-1	**Priority claim of earlier regional application**	
VI-1-1	Filing date	29 December 2017 (29.12.2017)
VI-1-2	Number	17306977.4
VI-1-3	Regional Office	EP
VI-2	**Priority document request**	
	The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as item(s):	VI-1
VI-3	**Incorporation by reference :**	
	where an element of the international application referred to in Article 11(1)(iii)(d) or (e) or a part of the description, claims or drawings referred to in Rule 20.5(a) is not otherwise contained in this international application but is completely contained in an earlier application whose priority is claimed on the date on which one or more elements referred to in Article 11(1)(iii) were first received by the receiving Office, that element or part is, subject to confirmation under Rule 20.6, incorporated by reference in this international application for the purposes of Rule 20.6.	
VII-1	**International Searching Authority Chosen**	European Patent Office (EPO) (ISA/EP)
VII-2	**Request to use results of earlier search; reference to that search**	
VII-2-1	Filing date	29 December 2017 (29.12.2017)
VII-2-2	Application Number	17306977.4
VII-2-3	Country (or regional Office)	EP
VII-2-4	Statement (Rule 4.12(ii)):	This international application is the same, or substantially the same, as the application in respect of which the earlier search was carried out except, where applicable, that it is filed in a different language.
VII-2-6	The applicant requests the receiving Office to prepare and transmit to the ISA a copy of the earlier search results (Rule 12bis.1(b) and (d)).	

PCT REQUEST

Print Out (Original in Electronic Form)

VIII	**Declarations**	Number of declarations	
VIII-1	Declaration as to the identity of the inventor	–	
VIII-2	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	–	
VIII-3	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	–	
VIII-4	Declaration of inventorship (only for the purposes of the designation of the United States of America)	–	
VIII-5	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	–	
IX	**Check list**	Number of sheets	Electronic file(s) attached
IX-1	Request (including declaration sheets)	5	✓
IX-2	Description	20	✓
IX-3	Claims	4	✓
IX-4	Abstract	1	✓
IX-5	Drawings	2	✓
IX-7	TOTAL	32	
	Accompanying Items	Paper document(s) attached	Electronic file(s) attached
IX-8	Fee calculation sheet	–	✓
IX-20	**Figure of the drawings which should accompany the abstract**	2	
IX-21	**Language of filing of the international application**	English	
X-1	**Signature of applicant, agent or common representative**	(PKCS7 Digital Signature)	
X-1-1	Name (LAST, First)	SCHEER, Luc	
X-1-3	Capacity (if such capacity is not obvious from reading the request)	(Representative)	

FOR RECEIVING OFFICE USE ONLY

10-1	**Date of actual receipt of the purported international application**	**19 NOV 2018 (19.11.2018)**
10-2	**Drawings:**	
10-2-1	Received	received
10-2-2	Not received	
10-3	**Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application**	
10-4	**Date of timely receipt of the required corrections under PCT Article 11(2)**	
10-5	**International Searching Authority**	**ISA/EP**
10-6	**Transmittal of search copy delayed until search fee is paid**	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	**Date of receipt of the record copy by the International Bureau**	

Based on USPTO Form PTO/SB/08

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Fabrice DELHOSTE
	Art Unit	
	Examiner Name	
	Attorney Docket Number	1032326-001016

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	20170109514	A1	2017-04-20	Cheng, et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2924603	EP	A2	2015-09-30	FMR LLC		☐
	2	2016083216	WO	A1	2016-06-02	GEMALTO SA		☐

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	International Search Report (PCT/ISA/210) and Written Opinion (PCT/ISA/237) mailed on January 22, 2019, by the European Patent Office as the International Searching Authority for International Application No. PCT/EP2018/081759.	☐

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

Based on USPTO Form PTO/SB/08

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Fabrice DELHOSTE
	Art Unit	
	Examiner Name	
	Attorney Docket Number	1032326-001016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document.
[4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e) (1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e) (2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James A LaBarre/	Date (YYYY-MM-DD)	2020-06-26
Name/Print	James A. LaBarre	Registration Number	28,632

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you

Based on USPTO Form PTO/SB/08

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Fabrice DELHOSTE
	Art Unit	
	Examiner Name	
	Attorney Docket Number	1032326-001016

require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
GMT3707WO/DD		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/EP2018/081759	19 November 2018 (19-11-2018)	29 December 2017 (29-12-2017)

Applicant

GEMALTO SA

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. [ ] **Certain claims were found unsearchable** (See Box No. II)
3. [ ] **Unity of invention is lacking** (see Box No III)
4. With regard to the **title**,
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:
5. With regard to the **abstract**,
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority
6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 2
      [X] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2018/081759

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/32 G06F21/35
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 2 924 603 A2 (FMR LLC [US]) 30 September 2015 (2015-09-30) abstract; figures 1-6 paragraph [0005] - paragraph [0012] paragraph [0035] - paragraph [0037] -----	1-15
A	WO 2016/083216 A1 (GEMALTO SA [FR]) 2 June 2016 (2016-06-02) abstract; figures 1-2 page 1, line 23 - page 4, line 16 -----	1-15
A	US 2017/109514 A1 (CHENG HUI [US] ET AL) 20 April 2017 (2017-04-20) abstract; figures 1-11 paragraph [0017] - paragraph [0031] -----	1-15

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 January 2019	22/01/2019

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Harms, Christoph

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2018/081759

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2924603 A2	30-09-2015	CA 2886136 A1	25-09-2015
		CN 105117622 A	02-12-2015
		EP 2924603 A2	30-09-2015
		JP 5856330 B2	09-02-2016
		JP 2015185175 A	22-10-2015
		US 8941741 B1	27-01-2015
WO 2016083216 A1	02-06-2016	EP 3026923 A1	01-06-2016
		WO 2016083216 A1	02-06-2016
US 2017109514 A1	20-04-2017	US 2016182503 A1	23-06-2016
		US 2017109514 A1	20-04-2017

Form PCT/ISA/210 (patent family annex) (April 2005)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP2018/081759	19.11.2018	29.12.2017

International Patent Classification (IPC) or both national classification and IPC
INV. G06F21/32 G06F21/35

Applicant
GEMALTO SA

1. This opinion contains indications relating to the following items:

- ☑ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☑ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Harms, Christoph Telephone No. +49 89 2399-0

Form PCT/ISA/237 (Cover Sheet) (January 2015)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☑ the international application in the language in which it was filed.

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:

   a. ☐ forming part of the international application as filed:

      ☐ in the form of an Annex C/ST.25 text file.

      ☐ on paper or in the form of an image file.

   b. ☐ furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.

   c. ☐ furnished subsequent to the international filing date for the purposes of international search only:

      ☐ in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).

      ☐ on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-15
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-15
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-15
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 **Independent Claims**

1 (method), 11 (apparatus), 13 (apparatus)

Independent claims 11 and 13 define the two authentication apparatuses deployed in the method of claim 1 and are thus allowable.

2 **Basis for amendments**

no amendments

3 **Prior art; Priority if applicable**

D1 EP 2 924 603 A2 (FMR LLC [US]) 30 September 2015 (2015-09-30)

D2 WO 2016/083216 A1 (GEMALTO SA [FR]) 2 June 2016 (2016-06-02)

D3 US 2017/109514 A1 (CHENG HUI [US] ET AL) 20 April 2017 (2017-04-20)

Only D1 teaches a video stream being captured by a camera 103 which is subsequently decomposed into separate audio/video segments (cap 402, spoken password "Rosebud", plant 408 and cat 404).

4 **Novelty: distinguishing features**

- constituting (28), based on the at least one collected context data element, a data packet;
- generating (216), by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- sending the generated hash;
- generating (220), as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and

authenticating (...) based on the generated hash distance

5 **Inventive step:**

5.1 Closest prior art

D1 EP 2 924 603 A2 (FMR LLC [US]) 30 September 2015 (2015-09-30)

discloses

An authentication method (20) comprising:
- collecting (24), based on a predetermined authentication policy, at least one context data element;
(...)
- authenticating (224) successfully or not (223) (...), as an authentication step.

5.2 Technical effect and problem to be solved

Technical security effect: accuracy of authentication

The technical problem means how to modify the closest prior art D1 in order to achieve the specified security effect

5.3 Solution (computer security countermeasure)

constitution of the data packets from the collected context data elements

hash type algorithm and hash distance generation as defined in the distinguishing features

5.4 Why is it inventive

D1 discloses a multi-factor authentication system in which the user is authenticated using his biometrics (facial, body movement, gesture; USER in D1 Fig. 4) and his environment (scene objects cat 404 and plant 408 in D1 Fig. 4) and his knowledge (spoken password "Rosebud" 406 in D1 Fig. 4). The computing device calculates a total score (115 in D1 table 2) of all video segments (which individually define the user biometrics, the user environment or the user knowledge) which is compared against a reference total score (145 in D1 table 2); cf. D1 Table 2.

D1, however, does not disclose nor render obvious to deploy hash functions for this specific purpose nor does it compute hash distances for comparing the sampled audio/video segments with respective reference. D1 table 2 and paragraphs [0035]-[0037] relies on simple numeric comparisons when comparing the sampled audio/video segment against their reference values.

The scope of independent claim 11 does NOT (!!!) encompass the application of a standard hash on data (claim 11: context data element/s) because the data packet(s) first need to be "extracted" from the collected context data elements (see definition of the collect and constitute steps) before the hash is applied on the preprocessed data packet(s) (and not on the context data elements).

6 **Further Relevant Information (Art. 82, 83, 84, 52, 53)**

The two-part form of the independent claims is not appropriate because it would complicate the wording of the claims.

The above reasoning corresponds to that of the parental application EP17306977.4

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 924 603 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
30.09.2015 Bulletin 2015/40

(51) Int Cl.:
G06F 21/32 *(2013.01)* ***G06K 9/00*** *(2006.01)*
G10L 17/00 *(2013.01)*

(21) Application number: **15160817.1**

(22) Date of filing: **25.03.2015**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
MA

(30) Priority: **25.03.2014 US 201414224901**

(71) Applicant: **FMR LLC**
Boston, MA 02210 (US)

(72) Inventors:
- **McDonough, John**
  Boston, MA 02210 (US)
- **Hromi, Jonathan**
  Boston, MA 02210 (US)
- **Stern, Hadley Rupert**
  Boston, MA 02210 (US)
- **Bisikalo, Dmitry**
  Boston, MA 02210 (US)

(74) Representative: **Greene, Simon Kenneth**
Elkington and Fife LLP
Prospect House
8 Pembroke Road
Sevenoaks, Kent TN13 1XR (GB)

(54) METHOD AND SYSTEM FOR USER AUTHENTICATION BASED ON BIOMETRICS, CLOTHES WEARING AND SURROUNDING SCENE

(57) Methods and apparatuses, including computer program products, are described for authentication using a video signature. A computing device receives a request to access a secure resource, and the request includes a first video segment comprising a plurality of visual and audio elements, wherein at least a first one of the visual elements comprises a physical characteristic of the user, e.g. biometrics, at least a second one of the visual elements comprises a physical object in proximity to the user, e.g. an object worn / owned by the user, and at least a third one of the visual elements comprises an element of the environment surrounding the user, e.g. determining geolocation. The computing device analyzes one or more of the plurality of visual and audio elements in the first video segment to determine a value associated with each of the one or more analyzed elements. The computing device calculates a total score for the first video segment based upon the value associated with each of the one or more analyzed elements. The computing device compares the total score for the first video segment to a score associated with a second video segment associated with the computing device. The computing device determines whether access to the secure resource is permitted based upon the comparison step.

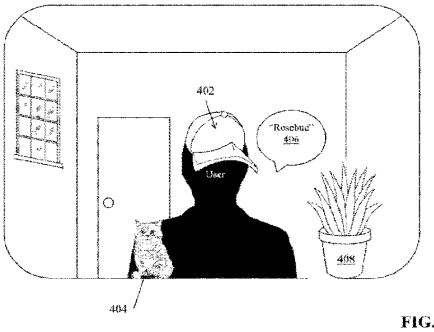


FIG. 4

EP 2 924 603 A2

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] This application relates generally to methods and apparatuses, including computer program products, for authentication using a video signature.

[0002] Typical authentication mechanisms, such as username / password combinations, are susceptible to theft, spoofing, phishing, and other forms of fraudulent activity by impostors seeking access to a user's secure accounts or resources (e.g., websites, documents, databases). More robust authentication techniques, like biometric scanning, have not yet become widely available and can depend significantly on both the type of technology available to a user and the type of technology used by an entity monitoring access to a secure resource.

[0003] Many computing devices, especially mobile devices, are equipped with cameras that can be used to record and transmit video segments (e.g., still images, video clips). Video segments typically incorporate a variety of visual and audio elements that can be used to uniquely identify the video segment in question from other video segments.

[0004] Therefore, what is needed are methods and systems to leverage the video capture capability of computing devices to generate a video signature used in authenticating a user and/or computing device to a secure resource. The techniques described herein provide the advantage of generating a video signature through analysis of a user-created and submitted video segment that includes a plurality of distinct visual and audio elements, where the plurality of elements are analyzed to calculate a total score for the video segment. A video segment, submitted by a user and assigned a score, can be used as a video signature to authenticate subsequent attempts to access the secure resource, e.g., by comparing the visual and audio elements in a later-submitted video segment against the video signature associated with a previously-submitted video segment.

[0005] The invention, in one aspect, features a method for authentication using a video signature. A computing device receives a request to access a secure resource, and the request includes a first video segment comprising a plurality of visual and audio elements. The computing device analyzes one or more of the plurality of visual and audio elements in the first video segment to determine a value associated with each of the one or more analyzed elements. The computing device calculates a total score for the first video segment based upon the value associated with each of the one or more analyzed elements. The computing device compares the total score for the first video segment to a score associated with a second video segment associated with the computing device. The computing device determines whether access to the secure resource is permitted based upon the comparison step.

[0006] The invention, in another aspect, features a system for authentication using a video signature. The system includes a computing device configured to receive a request to access a secure resource, and the request includes a first video segment comprising a plurality of visual and audio elements. The computing device is configured to analyze one or more of the plurality of visual and audio elements in the first video segment to determine a value associated with each of the one or more analyzed elements. The computing device is configured to calculate a total score for the first video segment based upon the value associated with each of the one or more analyzed elements. The computing device is configured to compare the total score for the first video segment to a score associated with a second video segment associated with the computing device. The computing device is configured to determine whether access to the secure resource is permitted based upon the comparison step.

[0007] The invention, in another aspect, features a computer program product, tangibly embodied in a non-transitory computer readable storage medium, for authentication using a video signature. The computer program product includes instructions operable to cause a computing device to receive a request to access a secure resource, and the request includes a first video segment comprising a plurality of visual and audio elements. The computer program product includes instructions operable to cause the computing device to analyze one or more of the plurality of visual and audio elements in the first video segment to determine a value associated with each of the one or more analyzed elements. The computer program product includes instructions operable to cause the computing device to calculate a total score for the first video segment based upon the value associated with each of the one or more analyzed elements. The computer program product includes instructions operable to cause the computing device to compare the total score for the first video segment to a score associated with a second video segment associated with the computing device. The computer program product includes instructions operable to cause the computing device to determine whether access to the secure resource is permitted based upon the comparison step.

[0008] In a yet further aspect, the invention relates to a method for authentication using a video signature, the method comprising: receiving, by a computing device from a remote device associated with a user, a request to access a secure resource, the request including a first video segment comprising a plurality of visual and audio elements, wherein at least a first one of the visual elements comprises a physical characteristic of the user, at least a second one of the visual elements comprises a physical object in proximity to the user, and at least a third one of the visual elements comprises an element of the environment surrounding the user; determining, by the computing device, a plurality of characteristics associated with each of the plurality of visual and audio elements; assigning, by the computing device, a value to each of the characteristics based upon predetermined value information stored by the computing device; calculating, by the computing device, a total score for the first video segment based upon the value associated with each of the character-

Thales Exhibit 2001, Page 233 of 339
Okta v. Thales DIS France - IPR2026-00278

istics; comparing, by the computing device, the total score for the first video segment to a score associated with a second video segment previously received from the remote device; determining, by the computing device, whether to permit the remote device to access the secure resource based upon the comparison step; and connecting, by the computing device, the remote device to the secure resource if access is permitted.

[0009] Any of the above aspects can include one or more of the following features. In some embodiments, the analyzing step includes determining one or more characteristics associated with each of the one or more plurality of visual and audio elements, assigning a value to the characteristics based upon predetermined value information stored by the computing device, and storing the values for the characteristics. In some embodiments, the one or more characteristics include a position of a visual element, movement of a visual element, a color of a visual element, a type of a visual element, and an absence of a visual element. In some embodiments, the computing device performs a speech-to-text conversion on an audio element. In some embodiments, values are assigned to the characteristics based upon frequency of appearance within frames of the first video segment. In some embodiments, the predetermined value information is adjusted based upon preferences provided by a user of the computing device.

[0010] In some embodiments, the calculating step includes assigning a weight to one or more of the analyzed elements based upon a security profile at the computing device. In some embodiments, the comparing step further includes comparing the value associated with one of the analyzed elements in the first video segment to a value associated with an analyzed element in the second video segment, and determining a deviation value based upon the comparison of the analyzed element values. In some embodiments, the computing device aggregates the deviation value for the comparisons of each of the analyzed element values and determines whether the aggregated deviation value falls below a predetermined threshold.

[0011] In some embodiments, the plurality of visual and audio elements includes a visual representation of a user of the computing device. In some embodiments, the plurality of visual and audio elements includes an object in proximity to the user of the computing device. In some embodiments, the plurality of visual and audio elements includes a phrase spoken by the user of the computing device.

[0012] In some embodiments, the first video segment is captured using a camera connected to the computing device. In some embodiments, the computing device is a mobile device. In some embodiments, the secure resource is a website.

[0013] Other aspects and advantages of the invention will become apparent from the following detailed description, taken in conjunction with the accompanying drawings, illustrating the principles of the invention by way of example only.

[0014] The advantages of the invention described above, together with further advantages, may be better understood by referring to the following description taken in conjunction with the accompanying drawings. The drawings are not necessarily to scale, emphasis instead generally being placed upon illustrating the principles of the invention.

FIG. 1 is a block diagram of a system for authentication using a video signature, according to an embodiment of the invention.

FIG. 2 is a block diagram of a system for authentication using a video signature, according to an embodiment of the invention.

FIG. 3 is a flow diagram of a method for authentication using a video signature, according to an embodiment of the invention.

FIG. 4 is a diagram of an exemplary video segment to be analyzed to generate a video signature, according to an embodiment of the invention.

FIG. 5 is a diagram of an exemplary video segment to be authenticated using a video signature, according to an embodiment of the invention.

FIG. 6 is a diagram of another exemplary video segment to be authenticated using a video signature, according to an embodiment of the invention.

[0015] FIG. 1 is a block diagram of a system 100 for authentication using a video signature, according to an embodiment of the invention. The system 100 includes a client computing device 102, a camera device 103 coupled to client device 102, a communications network 104, a server computing device 106 that includes a video signature authentication module 108, and a database 110.

[0016] The client device 102 connects to the server computing device 106 via the communications network 104 in order to authenticate a video signature captured by the client device 102. Exemplary client devices include desktop computers, laptop computers, tablets, mobile devices, smartphones, and internet appliances. It should be appreciated that other types of computing devices that are capable of connecting to the server computing device 106 can be used without departing from the scope of invention. Although FIG. 1 depicts one client device 102, it should be appreciated that the system 100 can include any number of client devices.

[0017] A camera device 103 is coupled to client device 102. The camera device can be any type of digital video camera (e.g., webcam) that is capable of capturing and transmitting video images of the user and/or the client device 102. As will be described in greater detail below, the camera device is configured to capture images of the user and the area

Thales Exhibit 2001, Page 234 of 339
Okta v. Thales DIS France - IPR2026-00278

surrounding the user for purposes of performing authentication of the user and/or the client device. In some embodiments, the camera device 103 is embedded in the client device 102, for example, a smartphone with an integrated camera or a laptop computer with an integrated webcam. Although FIG. 1 depicts one camera device 103, it should be understood that the system 100 can include any number of camera devices.

[0018] The communication network 104 enables the client device 102 to communicate with the server computing device 106 in order to perform authentication procedures. The network 104 may be a local network, such as a LAN, or a wide area network, such as the Internet and/or a cellular network. In some embodiments, the network 104 is comprised of several discrete networks and/or sub-networks (e.g., cellular → Internet) that enable the client device 102 to communicate with the server computing device 106. It should be understood that the client device 102 can connect to the server computing device 106 via a wireless network (e.g., Bluetooth, WiFi, and so forth).

[0019] The server computing device 106 is a combination of hardware and software modules that authenticates a video signature captured by the client device 102 and enables access by the client device to a secure resource. The server computing device 106 includes a video signature authentication module 108. The module 108 is a hardware and/or software module that resides on the server computing device 106 to perform functions associated with authenticating the video signature provided by the client device 102. In some embodiments, the functionality of the module 108 is distributed among a plurality of computing devices. It should be appreciated that any number of computing devices, arranged in a variety of architectures, resources, and configurations (e.g., cluster computing, virtual computing, cloud computing) can be used without departing from the scope of the invention.

[0020] The system 100 also includes a database 110. The database 110 is coupled to the server computing device 106 and stores data used by the server computing device 106 to perform the video signature authentication functionality. The database 110 can be integrated with the server computing device 106 or be located on a separate computing device. An example database that can be used with the system 100 is MySQL™ available from Oracle Corp. of Redwood City, California.

[0021] FIG. 2 is a block diagram of a system 200 for authentication using a video signature, according to an embodiment of the invention. The system 200 of FIG. 2 is similar to the system 100 of FIG. 1; the system 200 includes client device 102, a camera device 103 coupled to client device 102, and a database 110. In FIG. 2, however, the client computing device 102 includes the video signature authentication module 108, enabling the client device to perform video signature authentication locally (i.e., without requiring traversal of the communications network 104 of FIG. 1). As shown in FIG. 2, the camera device 103 is embedded within the client device 102. It should be appreciated that other configurations of the client device 102 and camera device are contemplated within the scope of invention, such as a camera device 103 wirelessly connected to the client device 102.

[0022] FIG. 3 is a flow diagram of a method 300 for authentication using a video signature, using the system 100 of FIG. 1. It should be appreciated that the system 200 of FIG. 2 can also be used to perform the method 300 depicted in FIG. 3.

[0023] The server computing device 106 receives (302) a request to access a secure resource. In one example, a secure resource is a website or other service that is protected from public access and requires the submission and verification of authentication credentials by a user seeking access to the secure resource. The process of authenticating the user involves verifying the user's identity.

[0024] For example, a user of client device 102 can navigate to a financial institution's website in order to log in to his or her account. Typically, such websites require that the user provides a form of authentication credential (e.g., username/password, token, and the like) before the user is granted access to the secure portions of the website where account information is available. It should be appreciated that other types of secure resources (e.g., databases, files, software) are included within the scope of invention.

[0025] As described herein, instead of or in addition to traditional authentication credentials, the server computing device 106 receives a new type of credential: a video segment captured by the client device 102 (e.g., using camera device 103 coupled to client device 102). Because video segments are multifaceted (i.e., typically including visual and audio elements), they can advantageously be used to generate a video signature - that is, a collection of distinct visual and audio elements represented in the video segment that are used to identify the associated user and can be compared to other video segments submitted by the user to authenticate the user's identity and allow access to the system.

[0026] The request to access a secure resource includes the captured video segment which comprises a plurality of visual and audio elements. Continuing with the above example, upon reaching the login page of the financial institution's website, the client device 102 captures a video segment and transmits the video segment to the server computing device as part of the authentication process. In some embodiments, the video segment is a single frame (i.e., image) or set of frames of video data captured by the camera device 103 that is used by the server computing device 106 to authenticate the user and/or the client device 102. The video segment can include any number of visual and audio elements that, when analyzed together, comprise the video signature for the video segment.

[0027] FIG. 4 is a diagram of an exemplary video segment 400 to be analyzed to generate a video signature, according to an embodiment of the invention. As shown in FIG. 4, the video segment comprises a video of the user wearing a

Thales Exhibit 2001, Page 235 of 339
Okta v. Thales DIS France - IPR2026-00278

baseball cap 402, holding a cat 404, saying the word "Rosebud" 406, with a potted plant 408 in the corner of the room. Each of the visual and audio elements 402, 404, 406 and 408 are used by the system 100 during the video signature authentication process. In addition, other elements of the video segment can be used for authentication, such as the user himself, apparel that the user is wearing, elements of the room (e.g., door, window), and so forth. For example, the module 108 can use facial recognition techniques to analyze the user and the result of such facial recognition methodology can be used as part of the total score for the video segment (as described in greater detail below). Other examples include voice recognition technology to analyze the user's speech patterns, speech-to-text conversion technology to isolate audio cues and/or spoken words within the video segment, and motion detection technology to track movement of the user and/or objects within the scene of the video segment. For example, if the user nods his head during the video segment, the module 108 can analyze the speed, position, and timing of the head movement as part of the overall analysis process described below.

[0028] Continuing with the method 300 of FIG. 3, the video signature authentication module 108 of server computing device 106 analyzes (304) one or more of the plurality of visual and audio elements 402, 404, 406, 408 in the first video segment 400 to determine a value associated with each of the one or more analyzed elements. As can be appreciated, the module 108 uses image and audio analysis algorithms / techniques to extract the various visual and audio elements from the video segment. For example, the module 108 can extract the shape of the baseball cap 402 from the video segment (or a single image of the video segment) and compare it to a database (e.g., database 110) of known shapes to determine a match. The module 108 can also analyze other characteristics associated with the visual and audio elements as part of the authentication process - such as color, position, and movement. For example, the module 108 determines that the baseball cap 402 is green and is positioned on top of the user's head.

[0029] Also, one or more of the visual and audio elements in the video segment can be assigned multiple values based upon different characteristics of the respective element. For example, the module 108 assigns the baseball cap a first value based upon its color (e.g., green) and assigns the baseball cap a second value based upon its position (e.g., on top of the user's head).

[0030] In some embodiments, the module 108 assigns a numeric value to each of the visual and audio elements 402, 404, 406, 408 represented in the video segment during the analysis step. Table One below depicts exemplary values assigned to each of the visual and audio elements 402, 404, 406 and 408:

TABLE ONE

Visual / Audio Element	Assigned Value
Baseball cap	10
Green baseball cap	15
Baseball cap on user's head	20
Cat	10
White cat	15
Holding cat in right hand	20
Saying "Rosebud"	25
Potted plant	10
Plant in back corner of room	20
TOTAL SCORE	145

[0031] After analyzing the video segment, the server computing device 106 calculates (306) a total score for the first video segment 400 based upon the value associated with each of the one or more analyzed elements. As shown in the table above, the total score for the video segment 400 is 145, based upon the summation of the individual visual and audio elements analyzed by the module 108. In some embodiments, certain visual and/or audio elements are weighted differently according to a predetermined security profile selected by the user and/or assigned by the module 108. For example, a financial institution may want to weigh the audio element 406 more heavily in the total score than a visual element (e.g., 408) because the institution can utilize speech recognition technology to identify the user with great precision (e.g., it may be harder for an impostor to duplicate a video segment that includes an audio element spoken by the user).

[0032] The module 108 stores the video segment and the associated values for each of the analyzed visual and audio elements in a database 110. The module 108 associates the stored data as a video signature for the particular user that

Thales Exhibit 2001, Page 236 of 339
Okta v. Thales DIS France - IPR2026-00278

submitted the video segment. Thus, the first time a video segment is submitted for analysis by client device 102, the module 108 stores the video segment and associated values as the video signature against which future video segment submissions from the user / client device are compared, similar to a username / password combination provided by a user.

[0033] When a user subsequently attempts to authenticate and gain access to a secure resource after providing a video segment, the module 108 compares (308) the total score for the earlier-provided video segment (i.e., the video segment that has been analyzed and stored by the system as described above) to a score associated with a second video segment associated with the client device 102 and/or user in order to identify and authenticate the user. For example, during a subsequent request to authenticate to the server computing device 106 and access a secure resource, the client device 102 submits a new video segment which is then analyzed by the module 108 (as previously described). In order to successfully authenticate, the total score of the newly-submitted video segment as calculated by the module 108 meets or exceeds a predetermined threshold when compared to the previously-stored video segment (e.g., segment 400).

[0034] FIG. 5 is a diagram of an exemplary video segment 500 to be authenticated using a video signature, according to an embodiment of the invention. As shown in FIG. 5, the same user from FIG. 4 is present in the video segment. The video segment 500 includes a plurality of video and audio elements 502, 504, 506, 508: the user has an orange baseball cap 502 on top of his head, is holding a white cat 504 in his right hand, and is speaking the word "Roseburg" 506. Also, a potted plant 508 is positioned in the rear corner of the room.

[0035] The module 108 receives the video segment 500 from the client device 102 and analyzes the video segment 500 in the same manner as described previously. For example, the module 108 assigns a numeric value to each of the visual and audio elements 502, 504, 506, 508 represented in the video segment 500. During this process, the values assigned to the elements 502, 504, 506, 508 are further scaled by comparing them to the same elements 402, 404, 406, 408 as analyzed in the previously-stored video segment 400. Table Two below depicts exemplary values assigned to each of the visual and audio elements 502, 504, 506 and 508 and compared to the values previously assigned to the elements 402, 404, 406, 408 from the first video segment 400:

TABLE TWO

Visual / Audio Element (Second Video Segment)	Assigned Value	Visual / Audio Element (First Video Segment)	Assigned Value
Baseball cap	10	Baseball cap	10
Orange baseball cap	0	Green baseball cap	15
Baseball cap on user's head	20	Baseball cap on user's head	20
Cat	10	Cat	10
White cat	15	White cat	15
Holding cat in right hand	20	Holding cat in right hand	20
Saying "Roseburg"	10	Saying "Rosebud"	25
Potted plant	10	Potted plant	10
Plant in back corner of room	20	Plant in back corner of room	20
TOTAL SCORE	115	TOTAL SCORE	145

[0036] The module 108 determines a total score for the second video segment 500 to be one-hundred fifteen. The total score for the second video segment 500 is lower than the score for the previously-stored video segment 400 due to two main differences: a) the user is wearing an orange baseball cap, not a green cap; and b) the user is speaking the word "Roseburg" instead of "Rosebud." The differences result in the module 108 assigning a lower value to those two elements of the second video segment 500 (i.e., because they do not match the same characteristics of the elements as represented in the first video segment 400).

[0037] The module 108 determines (310) whether access to the secure resource is permitted based upon the comparison step. As shown in the table above, the module 108 determines that the total score for the second video segment 500 is within thirty points of the total score for the first video segment 400 (i.e., one-hundred fifteen to one-hundred forty-five). As a result, the module 108 can determine that the total score for the second segment 500 is sufficient to satisfy a predetermined threshold for permitting access to the secure resource. For example, the module 108 may determine that any total score for a submitted video segment that exceeds one hundred is sufficient to permit access.

[0038] In some embodiments, the user can provide certain scoring parameters or thresholds that provide some flexibility

Thales Exhibit 2001, Page 237 of 339
Okta v. Thales DIS France - IPR2026-00278

in the visual and audio elements required to be present in video segments submitted for authentication. For example, the user may prefer that the color of the baseball cap 402 is not used during the analysis and authentication process - so that he can wear any baseball cap he might have available and still be able to authenticate to the system.

[0039] In some embodiments, the module 108 evaluates each of the visual and audio elements individually as part of the determination process to calculate a deviation value for the respective elements. For example, the module 108 may determine that, because only two of the nine values for the visual and audio elements in the second video segment 500 fall more than ten points below the corresponding elements in the first video segment 400 (i.e., a deviation value of ten), the second video segment 500 is sufficient to authenticate the user / client device 102. In another example, the module 108 may require that every visual and audio element in the second video segment 500 fall within at least eight points of the corresponding element in the first video segment 400 in order to permit access to the secure resource. Table Three below depicts exemplary values assigned to each of the visual and audio elements 502, 504, 506 and 508 and compared to the values previously assigned to the elements 402, 404, 406, 408 from the first video segment 400, including a deviation value for each element comparison:

TABLE THREE

Visual / Audio Element (Second Video Segment)	Assigned Value	Visual / Audio Element (First Video Segment)	Assigned Value	Deviation Value
Baseball cap	10	Baseball cap	10	0
Orange baseball cap	0	Green baseball cap	15	15
Baseball cap on user's head	20	Baseball cap on user's head	20	0
Cat	10	Cat	10	0
White cat	15	White cat	15	0
Holding cat in right hand	20	Holding cat in right hand	20	0
Saying "Roseburg"	10	Saying "Rosebud"	25	15
Potted plant	10	Potted plant	10	0
Plant in back corner of room	20	Plant in back corner of room	20	0
TOTAL SCORE	115	TOTAL SCORE	145	

[0040] The aggregate deviation value between the elements of the two video segments is thirty, while the average deviation value is 3.33. In some examples, the module 108 can use the average deviation value to determine whether access to the secure resource is permitted while in other examples, the aggregated deviation value can be used. As can be appreciated, a variety of scoring and comparison techniques can be used without departing from the scope of the invention.

[0041] FIG. 6 is a diagram of another exemplary video segment 600 to be authenticated using a video signature, according to an embodiment of the invention. As shown in FIG. 6, the third video segment 600 includes a plurality of video and audio elements 604, 606, 608: a person is holding a white cat 604 in his left hand and is speaking the words "Play it again" 606. Also, a coat rack 608 is positioned in the rear comer of the room. The person in FIG. 6 is not wearing a hat.

[0042] The module 108 receives the third video segment 600 from the client device 102 and analyzes the video segment 600 in the same manner as described previously. For example, the module 108 assigns a numeric value to each of the visual and audio elements 604, 606, 608 represented in the video segment 600. During this process, the values assigned to the elements 604, 606, 608 are further scaled by comparing them to the same elements 402, 404, 406, 408 as analyzed in the previously-stored video segment 400. Table Four below depicts exemplary values assigned to each of the visual and audio elements 604, 606, 608 in video segment 600 and compared to the values previously assigned to the elements 402, 404, 406, 408 from the first video segment 400:

TABLE FOUR

Visual / Audio Element (Third Video Segment)	Assigned Value	Visual / Audio Element (First Video Segment)	Assigned Value
No baseball cap	0	Baseball cap	10
No baseball cap	0	Green baseball cap	15

Thales Exhibit 2001, Page 238 of 339
Okta v. Thales DIS France - IPR2026-00278

(continued)

Visual / Audio Element (Third Video Segment)	Assigned Value	Visual / Audio Element (First Video Segment)	Assigned Value
No baseball cap	0	Baseball cap on user's head	20
Cat	10	Cat	10
White cat	15	White cat	15
Holding cat in left hand	5	Holding cat in right hand	20
Saying "Play it again"	0	Saying "Rosebud"	25
Coat rack	0	Potted plant	10
Coat rack in back corner of room	5	Plant in back corner of room	20
TOTAL SCORE	35	TOTAL SCORE	145

[0043] The module 108 determines a total score for the third video segment 600 to be thirty-five. The total score for the third video segment 600 is significantly lower than the score for the previously-stored video segment 400 due to many differences between the two segments: a) the absence of a baseball cap, b) the cat positioned in the wrong hand, c) the person speaking the wrong phrase, and d) the wrong object being positioned in the corner of the room. In this example, an impostor may be trying to gain access to the secure resource by attempting to pass himself off as the user by submitting a fraudulent video segment (just as someone may attempt to learn a user's password by making attempts using random character strings). Because the total score for the third video segment 600 is far below the total score for the first video segment 400, the module 108 denies the request to access the secure resource and does not authenticate the person / client device 102 to the system.

[0044] In some embodiments, if the submitted video segment does not meet or exceed a predetermined threshold for permitting access to the secure resource, the module 108 can offer other authentication means to the user so that such access may be granted. For example, the module 108 can prompt the user and/or client device 102 for an auxiliary authentication credential (e.g., biometric information, device footprint, token, public/private key information, and the like) in order to verify the identity of the user.

[0045] The above-described techniques can be implemented in digital and/or analog electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. The implementation can be as a computer program product, i.e., a computer program tangibly embodied in a machine-readable storage device, for execution by, or to control the operation of, a data processing apparatus, e.g., a programmable processor, a computer, and/or multiple computers. A computer program can be written in any form of computer or programming language, including source code, compiled code, interpreted code and/or machine code, and the computer program can be deployed in any form, including as a stand-alone program or as a subroutine, element, or other unit suitable for use in a computing environment. A computer program can be deployed to be executed on one computer or on multiple computers at one or more sites.

[0046] Method steps can be performed by one or more processors executing a computer program to perform functions of the invention by operating on input data and/or generating output data. Method steps can also be performed by, and an apparatus can be implemented as, special purpose logic circuitry, e.g., a FPGA (field programmable gate array), a FPAA (field-programmable analog array), a CPLD (complex programmable logic device), a PSoC (Programmable System-on-Chip), ASIP (application-specific instruction-set processor), or an ASIC (application-specific integrated circuit), or the like. Subroutines can refer to portions of the stored computer program and/or the processor, and/or the special circuitry that implement one or more functions.

[0047] Processors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and any one or more processors of any kind of digital or analog computer. Generally, a processor receives instructions and data from a read-only memory or a random access memory or both. The essential elements of a computer are a processor for executing instructions and one or more memory devices for storing instructions and/or data. Memory devices, such as a cache, can be used to temporarily store data. Memory devices can also be used for long-term data storage. Generally, a computer also includes, or is operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data, e.g., magnetic, magneto-optical disks, or optical disks. A computer can also be operatively coupled to a communications network in order to receive instructions and/or data from the network and/or to transfer instructions and/or data to the network. Computer-readable storage mediums suitable for embodying computer program instructions and data include all forms of volatile and non-volatile memory, including by way of example semiconductor memory devices, e.g., DRAM, SRAM, EPROM, EEPROM, and flash memory devices; magnetic disks, e.g., internal hard disks or removable disks; magneto-optical disks; and optical

Thales Exhibit 2001, Page 239 of 339
Okta v. Thales DIS France - IPR2026-00278

disks, e.g., CD, DVD, HD-DVD, and Blu-ray disks. The processor and the memory can be supplemented by and/or incorporated in special purpose logic circuitry.

[0048] To provide for interaction with a user, the above described techniques can be implemented on a computing device in communication with a display device, e.g., a CRT (cathode ray tube), plasma, or LCD (liquid crystal display) monitor, a mobile device display or screen, a holographic device and/or projector, for displaying information to the user and a keyboard and a pointing device, e.g., a mouse, a trackball, a touchpad, or a motion sensor, by which the user can provide input to the computer (e.g., interact with a user interface element). Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback, e.g., visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic, speech, and/or tactile input.

[0049] The above described techniques can be implemented in a distributed computing system that includes a back-end component. The back-end component can, for example, be a data server, a middleware component, and/or an application server. The above described techniques can be implemented in a distributed computing system that includes a front-end component. The front-end component can, for example, be a client computer having a graphical user interface, a Web browser through which a user can interact with an example implementation, and/or other graphical user interfaces for a transmitting device. The above described techniques can be implemented in a distributed computing system that includes any combination of such back-end, middleware, or front-end components.

[0050] The components of the computing system can be interconnected by transmission medium, which can include any form or medium of digital or analog data communication (e.g., a communication network). Transmission medium can include one or more packet-based networks and/or one or more circuit-based networks in any configuration. Packet-based networks can include, for example, the Internet, a carrier internet protocol (IP) network (e.g., local area network (LAN), wide area network (WAN), campus area network (CAN), metropolitan area network (MAN), home area network (HAN)), a private IP network, an IP private branch exchange (IPBX), a wireless network (e.g., radio access network (RAN), Bluetooth, Wi-Fi, WiMAX, 3G, 4G, 4G LTE, 5G, general packet radio service (GPRS) network, HiperLAN), and/or other packet-based networks. Circuit-based networks can include, for example, the public switched telephone network (PSTN), a legacy private branch exchange (PBX), a wireless network (e.g., RAN, code-division multiple access (CDMA) network, time division multiple access (TDMA) network, global system for mobile communications (GSM) network), and/or other circuit-based networks.

[0051] Information transfer over transmission medium can be based on one or more communication protocols. Communication protocols can include, for example, Ethernet protocol, Internet Protocol (IP), Voice over IP (VOIP), a Peer-to-Peer (P2P) protocol, Hypertext Transfer Protocol (HTTP), Session Initiation Protocol (SIP), H.323, Media Gateway Control Protocol (MGCP), Signaling System #7 (SS7), a Global System for Mobile Communications (GSM) protocol, a Push-to-Talk (PTT) protocol, a PTT over Cellular (POC) protocol, Universal Mobile Telecommunications System (UMTS), 3GPP Long Term Evolution (LTE) and/or other communication protocols.

[0052] Devices of the computing system can include, for example, a computer, a computer with a browser device, a telephone, an IP phone, a mobile device (e.g., cellular phone, personal digital assistant (PDA) device, smart phone, tablet, laptop computer, electronic mail device), and/or other communication devices. The browser device includes, for example, a computer (e.g., desktop computer and/or laptop computer) with a World Wide Web browser (e.g., Chrome™ from Google, Inc., Microsoft® Internet Explorer® available from Microsoft Corporation, and/or Mozilla® Firefox available from Mozilla Corporation). Mobile computing device include, for example, a Blackberry® from Research in Motion, an iPhone® from Apple Corporation, and/or an Android™-based device. IP phones include, for example, a Cisco® Unified IP Phone 7985G and/or a Cisco® Unified Wireless Phone 7920 available from Cisco Systems, Inc.

[0053] Comprise, include, and/or plural forms of each are open ended and include the listed parts and can include additional parts that are not listed. And/or is open ended and includes one or more of the listed parts and combinations of the listed parts.

[0054] One skilled in the art will realize the invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. The foregoing embodiments are therefore to be considered in all respects illustrative rather than limiting of the invention described herein.

Claims

1. A method for authentication using a video signature, the method comprising:

receiving, by a computing device from a remote device associated with a user, a request to access a secure resource, the request including a first video segment comprising a plurality of visual and audio elements, wherein at least a first one of the visual elements comprises a physical characteristic of the user, at least a second one of the visual elements comprises a physical object in proximity to the user, and at least a third one of the visual

Thales Exhibit 2001, Page 240 of 339
Okta v. Thales DIS France - IPR2026-00278

elements comprises an element of the environment surrounding the user;
determining, by the computing device, a plurality of characteristics associated with each of the plurality of visual and audio elements;
assigning, by the computing device, a value to each of the characteristics based upon predetermined value information stored by the computing device;
calculating, by the computing device, a total score for the first video segment based upon the value associated with each of the characteristics;
comparing, by the computing device, the total score for the first video segment to a score associated with a second video segment previously received from the remote device;
determining, by the computing device, whether to permit the remote device to access the secure resource based upon the comparison step; and
connecting, by the computing device, the remote device to the secure resource if access is permitted.

2. The method of claim 1, further comprising:

storing, by the computing device, the values for each of the characteristics in a database coupled to the computing device.

3. The method of claim 2, wherein the plurality of characteristics includes at least two of:

a position of a visual element, movement of a visual element, a color of a visual element, a type of a visual element, and an absence of a visual element.

4. The method of any preceding claim, further comprising performing, by the computing device, a speech-to-text conversion on an audio element.

5. The method of any preceding claim, wherein the values are assigned to the characteristics based upon frequency of appearance within frames of the first video segment.

6. The method of any preceding claim, wherein the predetermined value information is adjusted based upon preferences received from the remote device.

7. The method of any preceding claim, wherein the calculating step includes assigning, by the computing device, a weight to one or more of the characteristics based upon a security profile at the computing device.

8. The method of any preceding claim, the comparing step further comprising:

comparing, by the computing device, the value associated with one of the characteristics in the first video segment to a value associated with a corresponding characteristic of the same element in the second video segment; and
determining, by the computing device, a deviation value based upon the comparison of the characteristic values.

9. The method of claim 8, further comprising:

aggregating, by the computing device, the deviation value for the comparisons of each of the characteristic values; and
determining, by the computing device, whether the aggregated deviation value falls below a predetermined threshold.

10. The method of any preceding claim, wherein the plurality of visual and audio elements include a phrase spoken by the user.

11. The method of any preceding claim, wherein the first video segment is captured using a camera connected to the remote device.

12. The method of any preceding claim, wherein the remote device is a mobile device.

13. The method of any preceding claim, wherein the secure resource is a website.

Thales Exhibit 2001, Page 241 of 339
Okta v. Thales DIS France - IPR2026-00278

14. A system for authentication using a video signature, the system comprising a computing device configured to:

receive, from a remote device associated with a user, a request to access a secure resource, the request including a first video segment comprising a plurality of visual and audio elements, wherein at least a first one of the visual elements comprises a physical characteristic of the user, at least a second one of the visual elements comprises a physical object in proximity to the user, and at least a third one of the visual elements comprises an element of the environment surrounding the user;
determine a plurality of characteristics associated with each of the plurality of visual and audio elements;
assign a value to each of the characteristics based upon predetermined value information stored by the computing device;
calculate a total score for the first video segment based upon the value associated with each of the characteristics;
compare the total score for the first video segment to a score associated with a second video segment previously received from the remote device;
determine whether to permit the remote device to access the secure resource based upon the comparison step; and
connect the remote device to the secure resource if access is permitted.

15. The system of claim 14, wherein the computing device is further configured to:

store the values for each of the characteristics in a database coupled to the computing device.

16. The system of claim 14 or 15, wherein the first video segment is captured using a camera connected to the remote device.

17. The system of claim 14, 15 or 16, wherein the remote device is a mobile device.

18. A computer program product, tangibly embodied in a non-transitory computer readable storage medium, for authentication using a video signature, the computer program product including instructions operable to cause a computing device to: carry out a method according to any of claims 1 to 13.

Thales Exhibit 2001, Page 242 of 339
Okta v. Thales DIS France - IPR2026-00278

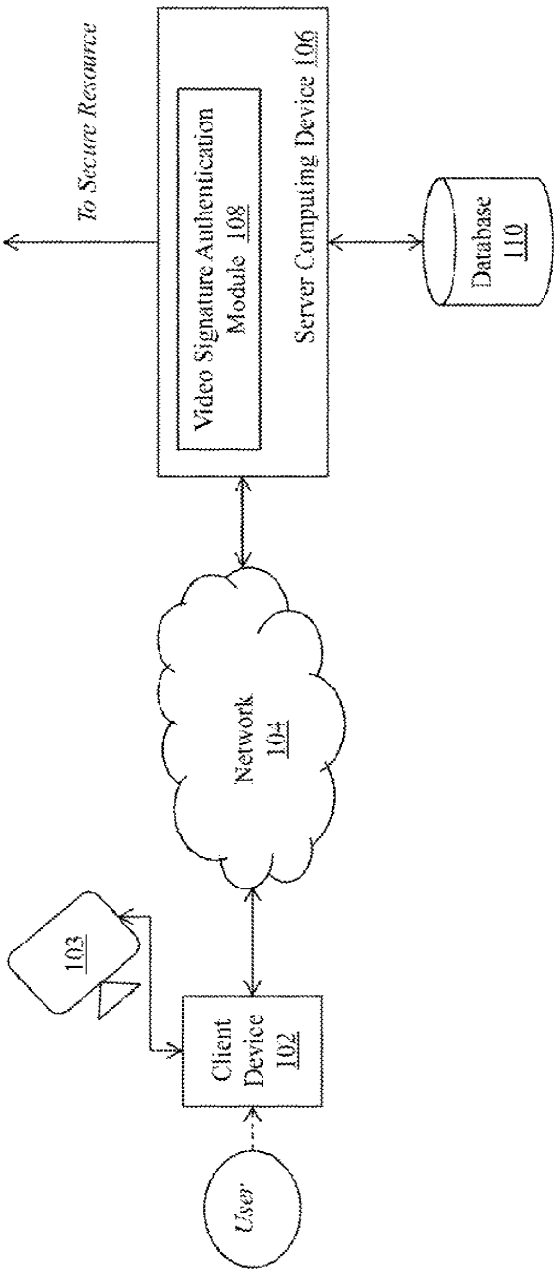


FIG. 1

Thales Exhibit 2001, Page 243 of 339
Okta v. Thales DIS France - IPR2026-00278

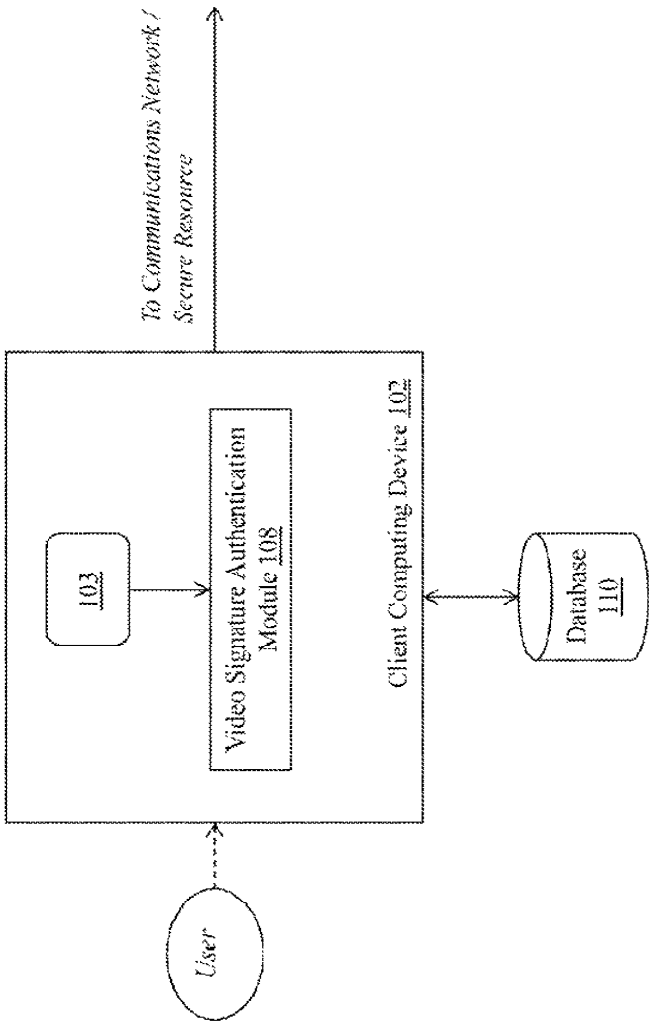


FIG. 2

Thales Exhibit 2001, Page 244 of 339
Okta v. Thales DIS France - IPR2026-00278

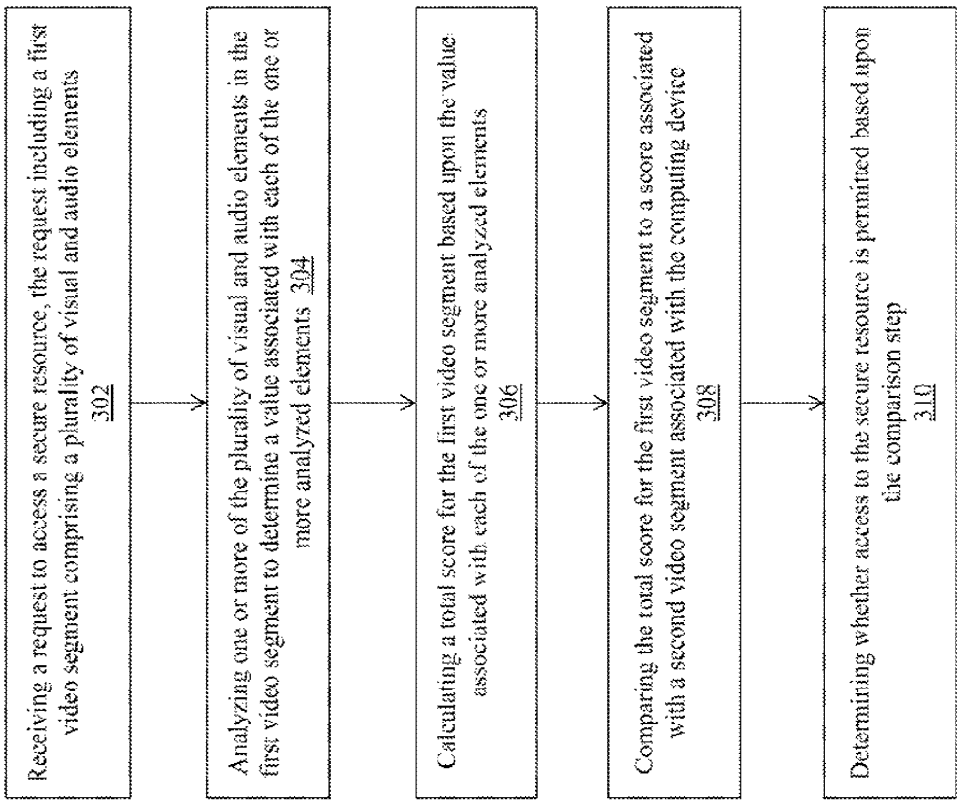


FIG. 3

Thales Exhibit 2001, Page 245 of 339
Okta v. Thales DIS France - IPR2026-00278

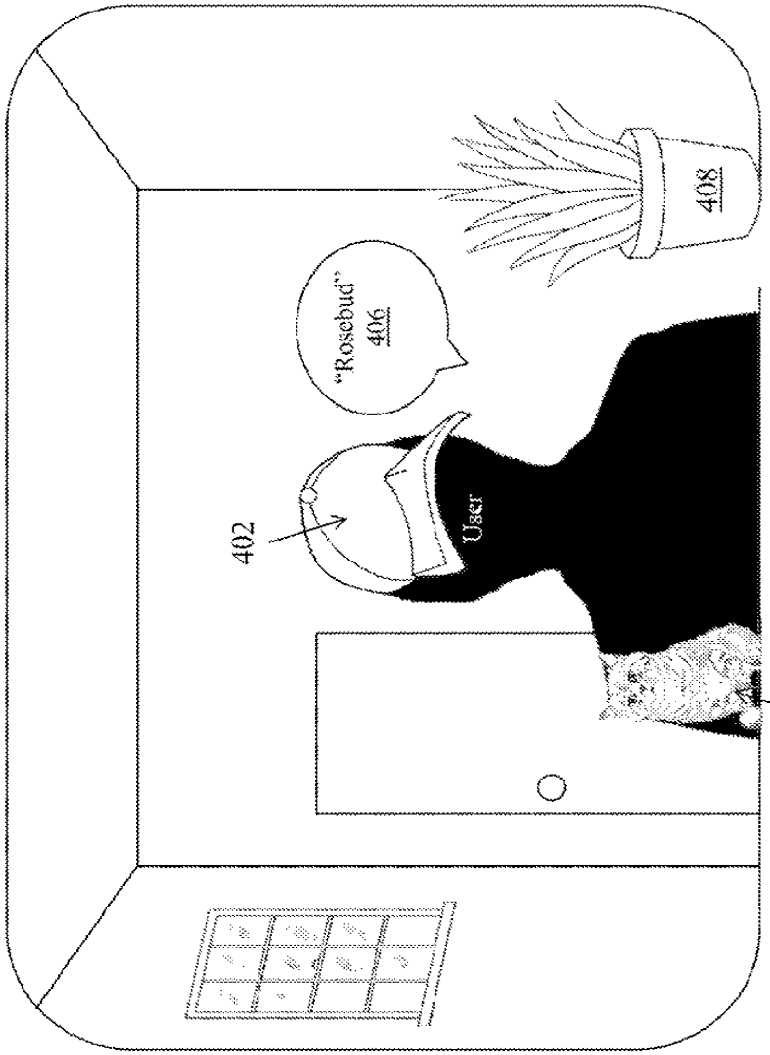


FIG. 4

Thales Exhibit 2001, Page 246 of 339
Okta v. Thales DIS France - IPR2026-00278

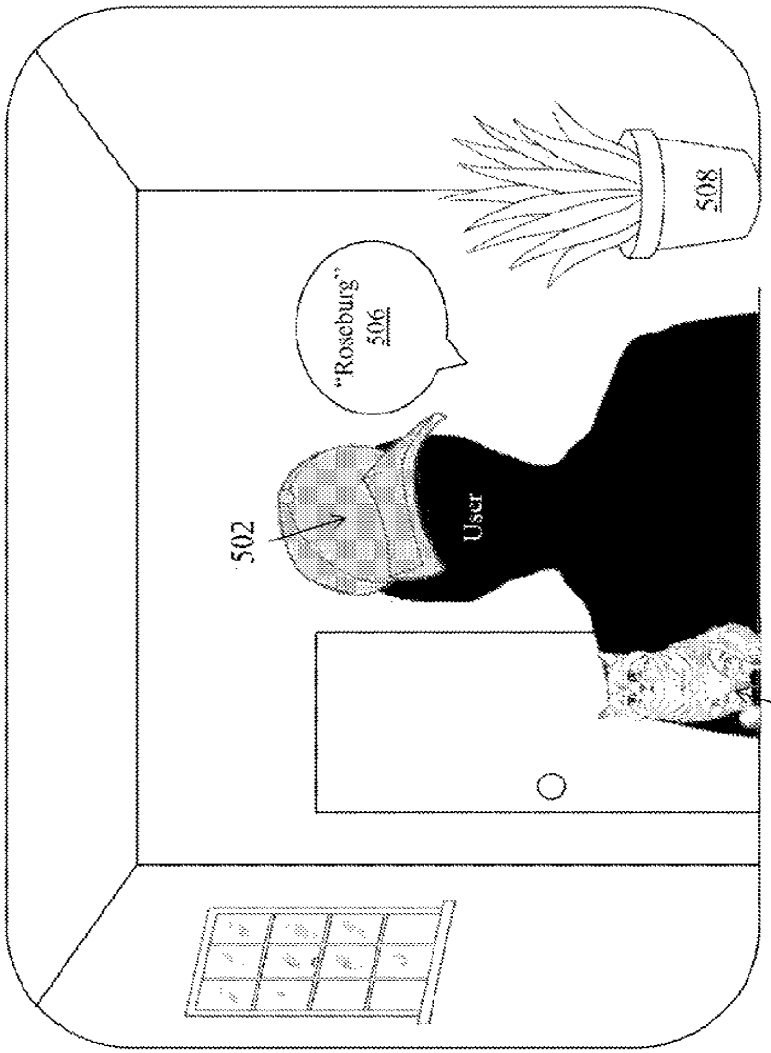


FIG. 5

Thales Exhibit 2001, Page 247 of 339
Okta v. Thales DIS France - IPR2026-00278

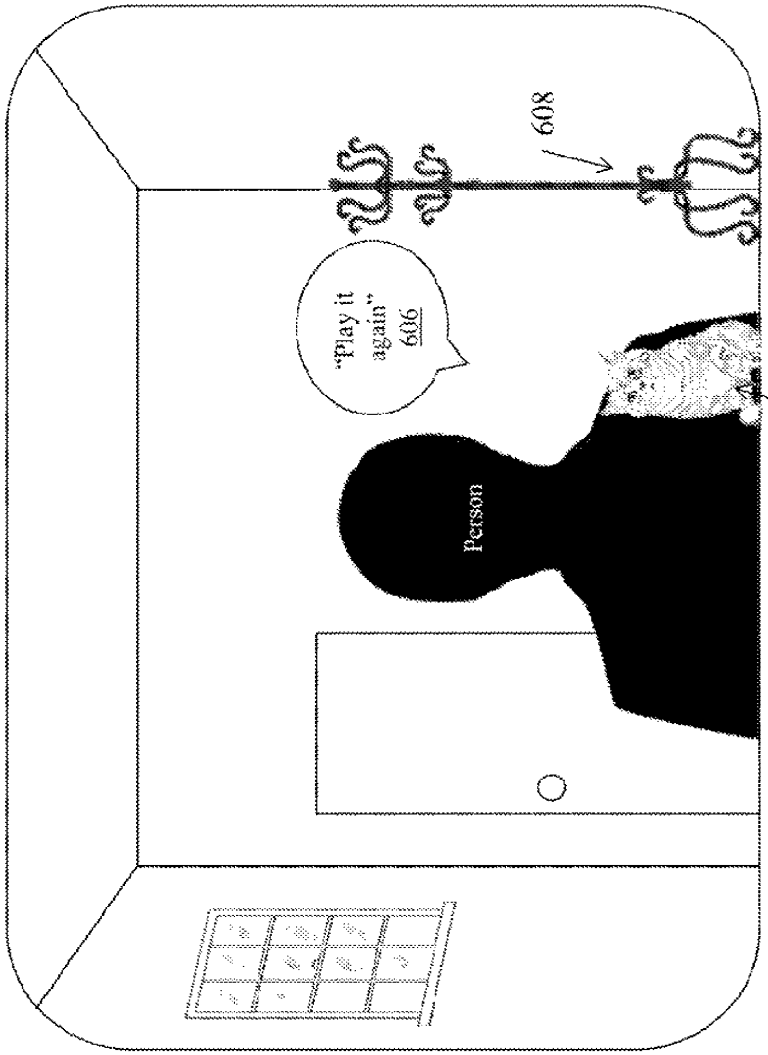


FIG. 6

Thales Exhibit 2001, Page 248 of 339
Okta v. Thales DIS France - IPR2026-00278

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 June 2016 (02.06.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/083216 A1

(51) International Patent Classification:
H04N 21/442 (2011.01) *H04N 21/4627* (2011.01)
H04N 21/45 (2011.01)

(21) International Application Number:
PCT/EP2015/077012

(22) International Filing Date:
18 November 2015 (18.11.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14306925.0 28 November 2014 (28.11.2014) EP

(71) Applicant: **GEMALTO SA** [FR/FR]; 6 rue de la Verrerie, 92190 Meudon (FR).

(72) Inventors: **PAILLART, Frédéric**; c/o GEMALTO SA, service brevets, 525 Avenue du Pic de Bertagne, CS12023, 13881 GEMENOS cedex (FR). **DELHOSTE, Fabrice**; c/o GEMALTO SA, service brevets, 525 Avenue du Pic de Bertagne, CS12023, 13881 GEMENOS cedex (FR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: METHOD FOR ACCESSING MEDIA DATA AND CORRESPONDING DEVICE AND SYSTEM

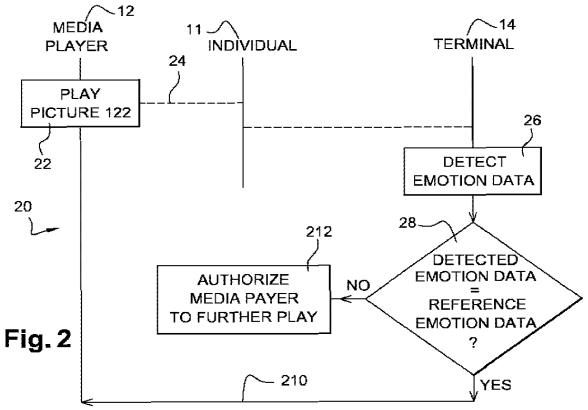


Fig. 2

(57) **Abstract**: The invention relates to a method 20 for accessing media data. - According to the invention, the method comprises the following steps. A first device 12 plays 22 media data content. The first device or a second device 14 detects 26, through at least one sensor, during the media data content play, at least one emotion presented 24 by at least one individual 11, the at least one individual listening and/or viewing the played media data content. The first device, the second device or a third device cooperating with the second device compares 28 the at least one detected emotion to at least one predetermined reference emotion for each concerned individual. The first, second or third device records, based upon the at least one emotion comparison result, an audience score relating to the at least one individual. The first, second or third device sends to a server the audience score. And the server decides, based upon the received audience score, to carry out at least one action. The invention also relates to corresponding device and system.

WO 2016/083216 A1

METHOD FOR ACCESSING MEDIA DATA AND CORRESPONDING DEVICE AND SYSTEM

Field of the invention:

The invention relates generally to a method for accessing media data.
Furthermore, the invention also pertains to a device for accessing media data.
Moreover, the invention relates to a system for accessing media data.

State of the art:

Nowadays, there are more and more videos and/or audios that are accessible via a TeleVision (or a TV) set, a radio set, a mobile (tele)phone or any other terminal.

However, a child may access a video (data) content and/or an audio (data) content, such as a war movie, an horror movie or the like, which is able to induce the child to respond negatively, i.e. while being scared.

Thus, there is a need to provide a solution that allows controlling access to audio and/or video (data) content that is experienced by a child who is able to respond or react negatively.

Summary of the invention:

The invention proposes a solution for solving the just herein above specified need by providing a method for accessing media data.

According to the invention, the method comprises the following steps. A first device plays media data content. The first device or a second device detects, through at least one sensor, during the media data content play, at least one emotion presented by at least one individual, the at least one individual listening and/or viewing the played media data content. The first device, the second device or a third device cooperating with the second device, as a control device, compares the at least one detected emotion to at least one predetermined reference emotion for each concerned individual. The control device decides, based upon at least one emotion comparison result, to carry out at least one action.

The principle of the invention consists in that, while a media content is played, a control device analyses whether a captured emotion of one (or several) individual(s) who experience(s) the media content is a predefined reference emotion to be tracked, for each concerned individual. In case the captured emotion is or is not a previously stored reference emotion, the control device decides to perform one or several actions.

The control device tracks thus an emotional response relating to each individual who consumes the media content and acts according to an emotion comparison result.

A tracked emotional response may be an emotional expression(s) and/or any emotional feature(s) of a body of the concerned individual.

It is noteworthy that the captured emotion and the reference emotion may be based on a static or a dynamic feature(s) of at least a part of the body of the concerned individual, like e.g. a picture or a series of pictures of a face of the concerned individual.

Since each individual interacts, i.e. exhibits an emotion, in real time with the play of the concerned media content, the control device also acts in real time.

It is to be noted that the invention does not impose any constraint with respect to the number and/or the type(s) of the predefined reference emotion(s). The reference emotion(s) may include, for each concerned individual, one or several pictures including a smile, a laugh, a fear and/or anger. Such a reference emotion(s) may be used as a reference emotion(s), expected and/or avoided.

Due to the fact that the control device assesses the captured emotion with respect to a predetermined reference emotion(s), the control device acts on the basis of a real experience relating to the concerned individual.

It is noteworthy that the invention does not impose any constraint with respect to the number and/or the type(s) of the action(s). The control device may thus carry out any number and/or any type of action(s).

The control device may rate the concerned media content based on an emotion comparison result for the concerned individual.

The control device may warn its user, other identified person(people) and/or a service provider, about a score obtained by a played media content that has been consumed by her/his child or another person(people), as individual(s). Such a score may help a media content provider, like e.g. an advertiser or a publisher, to enhance the media content, so as to increase its positive feedback and/or its audience.

For instance, if an individual(s) smile(s) or laugh(s), then the control device authorizes the individual(s) to further consume the played media content. Otherwise, i.e.

if an individual(s) is(are) scared, feared or angry, the control device forbids the individual to further continue consuming the played media content.

Thus, the invention solution allows a control device user to control access to a media (data) content for its audience, as individual(s), who consume(s) the concerned media content, in a quick, efficient and convenient manner.

Moreover, the invention solution allows a control device user to control access to a media (data) content specifically for the concerned individual(s), i.e. the action(s) may be adapted to the thus surveyed individual(s).

It is to be noted that the control device may be located at a place where the individual(s) consume(s) the media content or remotely, like e.g. in a network entity, from a distant server.

According to a further aspect, the invention is a device for accessing media data.

According to the invention, the device comprises means for playing a media data content. The device is configured to detect, through at least one sensor, during a media data content play, at least one emotion presented by at least one individual, the at least one individual listening and/or viewing the played media data content. The device is configured to compare, as a control device, the at least one detected emotion to at least one predetermined reference emotion for each concerned individual. The device is configured to decide, based upon at least one emotion comparison result, to carry out at least one action.

As device for accessing media data, it may be a media player equipped with one or several sensors, like e.g. a TV set equipped with a camera, a mobile terminal or glasses equipped with a camera, a display screen and/or an earphone(s).

According to still a further aspect, the invention is a system for accessing media data.

According to the invention, the system includes a first device and a second device. The first device comprises means for playing a media data content. The second device is configured to detect, through at least one sensor, during a media data content play, at least one emotion presented by at least one individual, the at least one individual listening and/or viewing the played media data content. The second device is configured to compare, as a control device, the at least one detected emotion to at least one predetermined reference emotion for each concerned individual. The second device is configured to decide, based upon at least one emotion comparison result, to carry out at least one action.

As a second device, it may a terminal, a user terminal, a token, a Secure Element (or SE) that cooperates with a host device, such as a media player or a terminal, or a remote server.

Within the present description, an SE is a smart object that, on the one hand, protects access to data that the smart object stores and, on the other hand, is intended to communicate with the outside world.

The SE may be embedded, like e.g. an embedded Universal Integrated Circuit Card (or eUICC) 14, within a host device, such as a mobile phone, as terminal.

Instead of being embedded, an SE chip may be included within a smart card termed Subscriber Identity Module (or SIM) type card or the like, as removable from its host device.

The invention does not impose any constraint as to a kind of the SE type. As removable SE, it may be a SIM type card, a Secure Removable Module (or SRM), a smart dongle of the USB (acronym for "Universal Serial Bus") type, a (micro-) Secure Digital (or SD) type card or a Multi-Media type Card (or MMC) or any format card to be coupled to a host device, as first device.

Brief description of the drawings:

Additional features and advantages of the invention will be more clearly understandable after reading a detailed description of one preferred embodiment of the invention, given as an indicative and non-limitative example, in conjunction with the following drawings:

- Figure 1 illustrates a simplified diagram of a mobile phone, as one exemplary embodiment of a local control device, the mobile phone being arranged to detect an emotion relating to an individual who consumes a played media content, to compare the detected emotion to a reference emotion(s) and to decide, based on an emotion comparison result, to carry out an action(s), according to the invention; and
- Figure 2 represents an example of one message flow between a media player, the individual and the mobile phone of figure 1, so that the mobile phone authorizes or forbids the individual to further consume the played media content.

Detailed description:

Herein under is considered a case in which the invention method for accessing media data is implemented by a TV set, as a media player and a first device, and a mobile phone, as a user terminal, a second device, a local control device and a standalone entity.

According to another embodiment, the invention method for accessing media data is implemented by a TV set, as a media player and a first device, a mobile phone, as a user terminal, and a remote server, as a third device and a remote control device. In other words, the mobile phone cooperates with the remote server, so as to decide, based on an emotion comparison result, to carry out an action(s). According to such an embodiment (not represented), the mobile phone is adapted to carry out a detection of an emotion of an individual that is described infra and that is performed by the mobile phone and the remote server is adapted to carry out a comparison of the detected emotion to a reference emotion(s) and to decide, based on an emotion comparison result, to carry out an action(s) that are described infra and that are performed by the mobile phone.

According to still another embodiment, the invention method for accessing media data is implemented by a TV set, as a media player and a first device, a mobile phone and a removable or incorporated SE, as a second device and a local control device. In other words, the SE cooperates with the mobile phone, so as to decide, based on an emotion comparison result, to carry out an action(s). According to such an embodiment (not represented), the SE is adapted to carry out the functions that are described infra and that are performed by the mobile phone.

Naturally, the herein below described embodiment is only for exemplifying purposes and is not considered to reduce the scope of the invention.

Figure 1 shows schematically an individual 11, a TV set 12, as a media player, and a mobile telephone 14, as a user terminal.

For the sake of simplicity, the TV set 12 and the mobile telephone 14 are termed herein after the TV 12 and the phone 14 respectively.

Only one individual 11 is represented. Nevertheless, the invention is also applicable to several individuals, the control device accesses, for each individual, one (or several) reference emotion(s) to be compared to each detected emotion prior to

deciding, based on an emotion comparison result, to carry out one or several actions, as further explained infra.

The TV 12, as a media player, plays e.g. a film, a TV-series, a video clip, a TV show or any other media data content.

The TV 12 may be compliant with Wifi, Bluetooth and/or any other Short Range (or SR) communication technology enabled.

Alternately or additionally, the TV 12 includes an infrared receiver.

Instead of a TV, the media player may be a Personal Computer (or a PC), a game player or any other device including means for reading media data and comprising or being connected to one or several user interfaces. As user interface(s), there may be a display screen(s) and/or a loudspeaker(s), so as to let view and/or listen the concerned media content.

Within the present description, media data is audio and/or video data.

The media data may originate, possibly through a set-top box, from a remote radio or TV transmitter, as a broadcaster, a Video On Demand (or VOD) provider, an Audio and Video On Demand (or AVOD) provider or any other remote provider(s) from a server (not represented).

The media data may originate from a local Digital Video Disk (or DVD) type player, a set-top box or any other local provider (not represented) that is connected to the TV 12.

An individual 11 is sufficiently close to the TV 12, so as to watch and listen, i.e. consume or experience, a media content that is being played by the TV 12.

The phone 14 is used for surveying the individual 11 who consumes a media content and may react or respond to the media content that is being played.

The individual 11 may thus smile, laugh, be angry and/or feared once or several times from a beginning of the play of the media content.

The individual 11 may be either a phone 14 user or a person distinct from a phone user, like e.g. a relative or a parent of the individual 11 or any person who desires to survey the individual 11.

Instead of a phone, it may be a PC, a tablet or any other device including means for processing data, comprising or being connected to means for storing data, and comprising or being connected to one or several sensors for capturing or detecting an emotion of the individual 11.

The phone 14 is preferably equipped with a camera(s) 142, as one sensor for capturing each emotion that is visually expressed by the individual 11. The camera 142 allows either filming continuously or taking regularly a picture of the individual 11 who is situated in front of the camera 142 and consumes a played media content.

Instead of being equipped with a camera, the phone 14 is connected to a camera (not represented).

The camera 142 that points the individual 11 is present e.g. on the front side of the phone 14.

Alternately, the camera 142 that points the individual 11 is on the rear side of the phone 14.

The camera 142 is used for detecting an (or a plurality of) emotion(s) that the invidual 11 presents by consuming the concerned played media content. To detect an emotion of the individual 11, the camera 142 may focus on a face of the individual 11, so as to extract either statically, i.e. through a picture, or dynamically, i.e. through a series of pictures, a facial expression. The facial expression may be based on an eye(s) expression and/or a mouth expression, as an individual body feature(s).

The phone 14 may be also equipped with (or connected to) a second camera (not represented), so as to either film continuously or take regularly a picture of the media content that is being played and consumed by the individual 11 in a manner synchronized with the operation of the first camera 142. The second camera is used for recording what the individual 11 watches at the time she/he has an emotion that is captured by the first camera 142. The phone 14 is thus able to associate a captured emotion with the corresponding played media content, like e.g. a picture or a series of pictures, as an extract of the consumed played media content that allows getting an emotional expression(s) from the individual 11.

The phone 14 is preferably equipped with one (or several) microphone(s) 144, as a sensor(s) for capturing each emotion that is orally expressed by the individual 11. The microphone 144 is used for detecting a sound(s), like e.g. a laughter sound(s) and/or a cry sound(s), as an emotion(s), that the invidual 11 produces by consuming the played media content.

The phone 14 may be provided with a bracelet (not represented) and/or another wearable device, as a biometric data reader and a sensor, that is used for capturing each emotion that is expressed by a feature(s) of the individual 11. To detect an emotion of the individual 11, the biometric data reader may measure or sense a body

temperature increase (associated with a fear), a ruffled fur (associated with a fear) and/or an increased heart rate (associated with a fear), as an individual body feature(s).

The phone 14 is preferably provided with wireless communication means for exchanging data with outside.

Within the present description, the adjective "wireless" denotes notably that the communication means communicates via one or several Long Range (or LR) and/or Short Range (or SR) Radio-Frequency (or RF) links.

The SR RF link may be related to a Wifi or Bluetooth type link.

Alternately or additionally, the wireless communication means includes an infrared transmitter.

The phone 14 includes one or several microprocessors (not represented), as data processing means, one or several memories (not represented), data storing means, and two or more Input/Output (or I/O) interfaces.

The phone memory(ies) may comprise one or several volatile memories and/or one or several non-volatile memories.

The phone memory stores an Operating System (or OS) and one or several applications to be executed by the phone microprocessor. The applications including the invention application are offered to the phone 14 user.

The phone memory stores preferably one (or several) predetermined picture(s) 140 that includes a laugh of the individual 11, as a reference emotion(s), that may be expected. Such a picture 140 presents, for instance, an individual 11 face that has a relatively narrow eye opening and/or a mouth that is open with lip corners that are pulled obliquely.

The phone memory may store one (or several) predetermined picture(s) that include(s) a smile of the individual 11, as a reference emotion(s).

The phone memory stores preferably one (or several) predetermined picture(s) 141 that include(s) a fear of the individual 11, as a reference emotion(s), that may be feared or avoided. Such a picture 141 presents, for instance, an individual 11 face that has a relatively large eye opening and/or a mouth that is frankly open with lip corners that are pulled vertically.

The phone memory may store one (or several) predetermined picture(s) that include(s) anger of the individual 11, as a reference emotion(s).

The phone memory may store data relating to a Uniform Resource Identifier (or URI), a Uniform Resource Locator (or URL) and/or an Internet Protocol (or IP) address

of an external entity to be addressed, like a server, as a device that collects each detected emotion and/or a corresponding audience score.

The phone 14 may be arranged to detect that a media content is being played and/or the individual 11 is present in front of the phone 14, as an incoming event(s), so as to awake automatically the invention application to survey the concerned individual 11.

The phone 14 is configured to detect, through one or several sensors, each emotion presented by the individual 11. Then, the phone 14 records preferably each detected emotion within the phone memory.

At the time an emotion is detected, the invention application may allow recording, within the phone memory, the associated media content that is being played.

The phone 14 is configured to analyse each emotion that is detected through the sensor(s) and that originates from the concerned individual 11 during a media content play.

To analyse the detected emotion, the invention application allows comparing each detected emotion to one or several pre-stored reference emotions that are accessible. Such a reference emotion(s) to be used is(are) entered, configurable and selected under the phone user control.

The invention application allows deciding, based on a result of one or several comparisons to the reference emotion(s), to carry out one or several actions.

The actions may be of different natures.

As actions, it may include an authorization or an interdiction to further play part or all of the media content that is being played.

Alternately or additionally, it may include an analysis of the result of the comparison(s) to the reference emotion(s), so as to allocate a score, as an audience score, to each of the concerned individual 11 who consumes the media content. The invention application allows recording each audience score. The invention application may allow sending each audience score to a central server. The server may thus decide, based on the received audience score, possibly further to a comparison of an average of all the received audience scores to a predetermined reference audience score, like e.g. an expected audience score, to carry out one or several actions.

The invention application may allow transmitting to an identified device(s), like e.g. a mobile phone, a message for warning its user, every time a detection of a predetermined emotion, like e.g. a fear or anger, occurs.

The invention application may allow transmitting wirelessly to an identified device, like e.g. the TV 12, a message including a command for switching off the media content that is being played and/or the TV 12 or a command for switching from a TV 12 source of the played media content to a predetermined targeted source, like e.g. a dedicated child program content provider, as a local or remote content provider, so as to stop the play of the media content.

Figure 2 depicts an exemplary embodiment of a message flow 20 that involves the TV 12, the individual 11 and the phone 14.

It is assumed that the phone 14 user, as a parent of a child, as the individual 11, desires to either authorize or forbid the child 11 to follow a TV program, as a media content, that is being played by the TV 12.

It is assumed that only the camera 142 is used as the sensor for detecting an emotion presented or expressed by the child 11. It is clear that (an)other sensor(s) may be used for detecting an emotion. In such a case, a corresponding digital template is associated with each used sensor. For instance, a microphone is used and a pre-stored reference sound is to be tracked and the phone 14 is configured to compare each detected sound to the reference sound. Furthermore, in order to enhance the recognition of a particular reference emotion, like e.g. a fear, several sensors, like e.g. the camera 142 and the microphone 144 are used and the detected picture and the detected sound are both compared to the reference emotion picture and the reference emotion sound respectively. For each used sensor type, there is an associated digital template type.

It is further assumed that the phone 14 stores the picture 141 that includes a fear of the child 11, as a fear picture 141 and reference emotion that is negative and to be avoided. The reference emotion 141 has been either loaded into the phone 14 or acquired with the phone camera 142.

The phone 14 user launches an execution of the invention application after having placed the phone 14 between the child 11 and the TV 12, so as to observe any feedback or response of the child 11 to be surveyed.

The child 11 consumes, i.e. views and/or listens to, the TV program.

At a given time, the TV program includes a picture 122 that is frightening for the child 11, like e.g. an animal with a ferocious air and extremely big teeth.

The TV 12 plays 22 the frightening picture 122.

The played frightening picture 122, as played media content, causes 24 a fear emotional state of the child 11.

The phone 142 detects 26, through the camera 142, during the media content play, a picture of the fear emotional state of the child 11, as detected emotion data.

Optionally, part or all the emotion (data) is detected, the phone 14 sends to a remote server (not represented) part or all of the detected emotion(s).

The phone 14 compares 28 the detected picture of the fear emotional state of the child 11 to the fear picture 141, as a reference emotion data.

If the detected picture of the fear emotional state of the child 11 matches the fear picture 141, then the phone 14 decides, based on the emotion comparison result, to forbid to further play the TV program by e.g. stopping the play of the TV program. To stop the play of the TV program, the phone 14 sends wirelessly to the TV 12 a message 210 including a command for switching off the TV program that is being played and/or the TV 12 or a command for switching from a TV 12 source of the played TV program to a predetermined targeted source, like e.g. a dedicated child content provider, as a local or remote content provider.

Optionally, instead of a single detection of the fear picture 141, a predetermined threshold, like e.g. three, possibly during a predefined period of time, such as two or three minutes, is or are to be reached prior to deciding to forbid to further play the TV program by e.g. stopping the play of the TV program.

Such an interdiction of the play of the TV program prevents its audience from continuing to consume the concerned TV program with a frightening picture(s), violent picture(s), dangerous scene(s)....

Otherwise, i.e. while the detected emotion data relating to the child 11 does not match any (tracked) reference emotion data, the phone 14, as control device, authorizes 212 the TV 12, as media player, to further play part or all the TV program.

Alternately or additionally, instead of authorizing or forbidding to further play the media content, the phone 14 records, based on the emotion comparison result, an audience score relating to child 11. The phone 14 may send to a remote server (not represented) the audience score. The server may collect from a fleet of control devices, like e.g. the phone 14, an audience score for the played TV program. The server decides, based on the received audience score(s), to carry out one or several actions, like e.g. an authorization or an interdiction of a server, as the provider of the concerned media content, to further play part or all the media content.

The invention allows thus a phone user who desires to survey an individual to control access in real time to the played media content specifically for the surveyed individual. As a matter of fact, for one and the same media content, a first child may react positively while a second child may react negatively.

The invention is therefore quick, efficient, convenient for a control device user.

The embodiment that has just been described is not intended to limit the scope of the concerned invention. Other embodiments may be given. As another embodiment example, instead of having two or three separate devices that are involved, one and the same device, such as e.g. a mobile terminal, a TV or glasses, that is equipped with a media player and comprises or is connected to one or several sensors, carries out the function that is performed by the TV 12 and the functions that are performed by the phone 14 that are all described supra.

CLAIMS

1. A method (20) for accessing media data,
characterized in that the method comprises the following steps:
- a first device (12) plays (22) media data content;
- the first device or a second device (14) detects (26), through at least one sensor, during the media data content play, at least one emotion presented (24) by at least one individual (11), the at least one individual listening and/or viewing the played media data content;
- the first device, the second device or a third device cooperating with the second device, compares (28) the at least one detected emotion to at least one predetermined reference emotion for each concerned individual;
- the first, second or third device records, based upon the at least one emotion comparison result, an audience score relating to the at least one individual;
- the first, second or third device sends to a server the audience score; and
- the server decides, based upon the received audience score, to carry out at least one action.

2. Method according to claim 1, wherein, the at least one reference emotion being associated with an authorization or an interdiction to consume the media data content, the at least one action comprises an authorization (212) or an interdiction of the first device to further play at least a part of the media data content.

3. Method according to any previous claim, wherein the first, second or third device records the at least one detected emotion and/or the associated extract of the played media data content.

4. Method according to any previous claim, wherein the first, second or third device sends to a server at least one of the at least one detected emotion.

5. Method according to any previous claim, wherein the at least one sensor comprises at least one element of a group including:
- at least one camera (142);
- at least one microphone (144); and
- at least one biometric data reader.

6. Method according to any previous claim, wherein the at least one reference emotion comprises at least one element of a group including:
- at least one predetermined picture including a smile relating to each of the at least one individual;
- at least one predetermined picture (140) including a laugh relating to each of the at least one individual;
- at least one predetermined picture (141) including a fear relating to each of the at least one individual; and
- at least one predetermined picture including anger relating to each of the at least one individual.

7. A device for accessing media data,
characterized in that, the device comprising means for playing a media data content, the device is configured to:
- detect, through at least one sensor, during a media data content play, at least one emotion presented by at least one individual, the at least one individual listening and/or viewing the played media data content;
- compare the at least one detected emotion to at least one predetermined reference emotion for each concerned individual;
- record, based upon the at least one emotion comparison result, an audience score relating to the at least one individual; and
- send to a server the audience score.

8. Device according to claim 7, wherein the device includes a mobile phone.

9. A system for accessing media data,
characterized in that, the system including a first device (12), a second device (14) and a server, the first device comprising means for playing a media data content, the second device is configured to:
- detect (26), through at least one sensor (142, 144), during a media data content play, at least one emotion presented (24) by at least one individual (11), the at least one individual listening and/or viewing the played media data content;

- compare (28) the at least one detected emotion to at least one predetermined reference emotion for each concerned individual;
- record, based upon the at least one emotion comparison result, an audience score relating to the at least one individual;
- send to the server the audience score; and

in that the server is configured to decide, based upon the received audience score, to carry out at least one action.

10. Device according to claim 9, wherein the first device includes a media player.

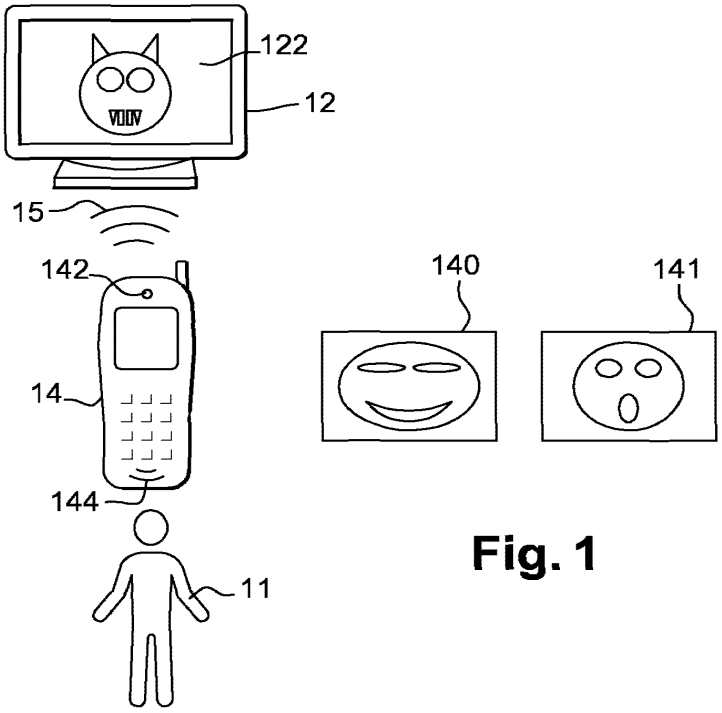

122
12
15
142
14
144
11
140
141

Fig. 1

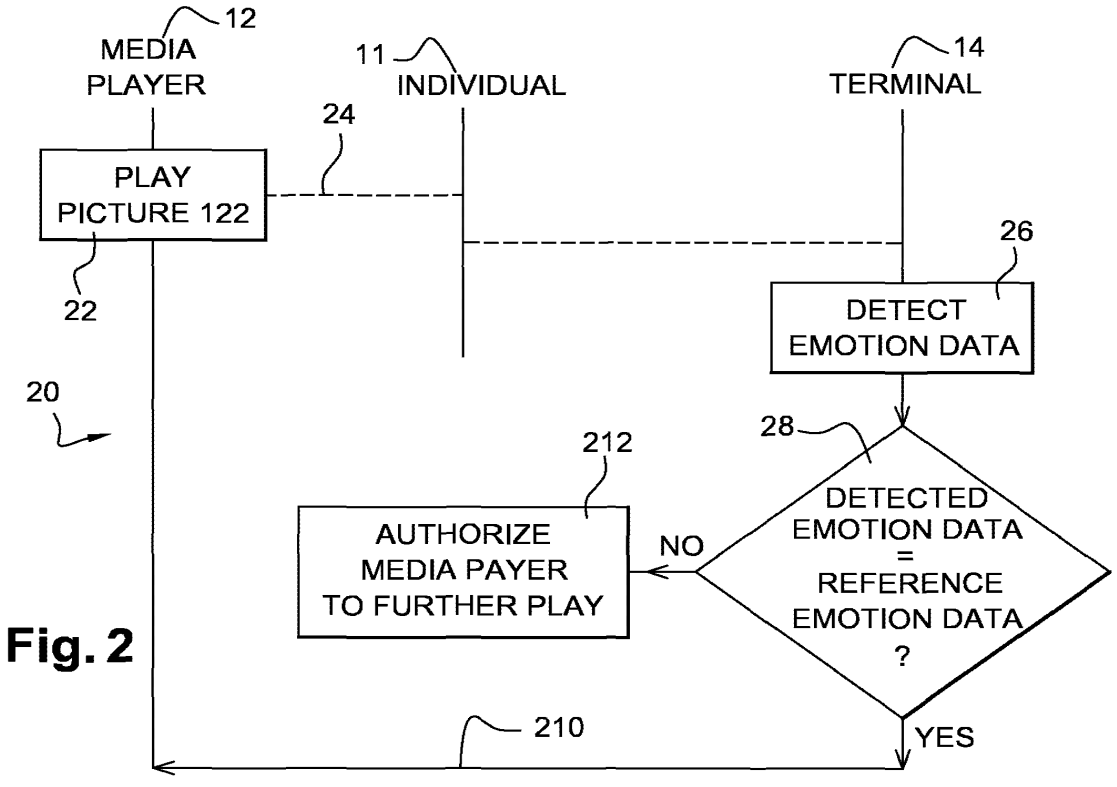

12
MEDIA PLAYER
11
INDIVIDUAL
14
TERMINAL
24
PLAY PICTURE 122
22
26
DETECT EMOTION DATA
20
28
212
AUTHORIZE MEDIA PAYER TO FURTHER PLAY
NO
DETECTED EMOTION DATA = REFERENCE EMOTION DATA ?
210
YES

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/077012

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04N21/442 H04N21/45 H04N21/4627
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2012/124456 A1 (PEREZ KATHRYN STONE [US] ET AL) 17 May 2012 (2012-05-17) paragraphs [0019], [0033] - [0042], [0046], [0065], [0066]; figures 1,2	1-10
Y	US 2014/025620 A1 (GREENZEIGER MICHAEL FROIMOWITZ [US] ET AL) 23 January 2014 (2014-01-23) pages 3-6	1-10
Y	US 2013/080260 A1 (FRENCH PAUL B [IE] ET AL) 28 March 2013 (2013-03-28) pages 2,3	1-10
Y	US 2002/178440 A1 (AGNIHOTRI LALITHA [US] ET AL) 28 November 2002 (2002-11-28) page 2	1-10

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 January 2016	27/01/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Folea, Octavian

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/077012

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014/130076 A1 (MOORE STEPHEN [US] ET AL) 8 May 2014 (2014-05-08) pages 3-6	1-10

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/077012

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012124456 A1	17-05-2012	CA 2815919 A1	18-05-2012
		CN 102541257 A	04-07-2012
		EP 2638702 A2	18-09-2013
		JP 2014502454 A	30-01-2014
		KR 20130125367 A	18-11-2013
		US 2012124456 A1	17-05-2012
		WO 2012064565 A2	18-05-2012
US 2014025620 A1	23-01-2014	US 2014025620 A1	23-01-2014
		WO 2014018216 A1	30-01-2014
US 2013080260 A1	28-03-2013	GB 2494945 A	27-03-2013
		US 2013080260 A1	28-03-2013
US 2002178440 A1	28-11-2002	CN 1460371 A	03-12-2003
		EP 1374582 A1	02-01-2004
		JP 2004527954 A	09-09-2004
		KR 20030004447 A	14-01-2003
		US 2002178440 A1	28-11-2002
		WO 02080546 A1	10-10-2002
US 2014130076 A1	08-05-2014	NONE	

AUTHENTICATION METHOD, DEVICE AND SYSTEM

Field of the invention:

The present invention relates generally to an authentication method and an authentication device.

Furthermore, the invention pertains to an authentication system as well. The system includes at least two devices.

The present invention is notably applicable to a field in which a first device is e.g. a mobile (tele)phone or a Personal Computer (or PC) and a second device is e.g. a (local) Secure Element (or SE) or a remote server.

Within the present description, an SE is a smart object that includes a chip(s) that protect(s), as a tamper resistant component(s), access to stored data and that is intended to communicate data with a device(s), like e.g., an SE host device, and/or an SE user.

State of the art:

EP 2 924 603 A2 describes a user authentication technique based on a transmission, from a client to a server, of a captured video signal including a physical user characteristic(s) and a physical object(s)/element(s) in the user environment. The sever analyses the captured video signal to determine a value associated with each of the visual and audio elements, as environment characteristics. The server determines a total score for the captured video signal and compares the total score to a predetermined reference score. The server decides to authorize (or not) based on a comparison result.

However, such a known solution requires a big bandwidth, namely several Mb, for an upload of the captured video signal. Moreover, the uploaded captured video signal includes information that discloses the user environment and therefore private data.

There is a need of an alternative authentication solution while being more efficient and more secure than such an aforementioned known solution.

Summary of the invention:

The invention proposes a solution for satisfying the just herein above specified need by providing an authentication method.

According to the invention, the method comprises:

- collecting, based on a predetermined authentication policy, at least one context data element;

- constituting, based on the at least one collected context data element, a data packet;
- generating, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- sending the generated hash;
- generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and
- authenticating successfully or not based on the generated hash distance, as an authentication step.

The principle of the invention consists in capturing, at a client device side, (local) context (or environment) data element(s) depending on an authentication policy, building a corresponding data packet and determining with a predefined hash type algorithm and, as input, the data packet a corresponding hash. The client device sends the determined hash. Then, a hash distance between the determined hash and a predefined reference hash is determined. The thus determined hash distance is then used for authenticating (or not) the tested authentication context (under survey).

The authentication policy defines notably the number and/or the nature of the context data element(s) to be captured. The authentication policy may include data relating to the used (client) device, a user, object(s) or thing(s) to be locally present and detected. To capture the context data element(s), the invention does not impose any constraint. The client device may use a camera(s), a microphone(s) and/or one or several sensors that is(are) incorporated within or connected to the client device.

The invention (authentication) solution is, through the authentication policy, configurable and therefore adaptable to different (local) environment or context scenario(s).

Since the client device (or a cooperating device, such as an SE), where there is an environment to be authenticated, generates (or determines) a hash from a data packet resulting from captured environment or context data element(s), the hash is transmitted in a secure and protected manner.

A software component, such as a library, a hardware component and/or a device may carry out the hash distance generation step and the authentication step. The software component may be supported by the client device, a local device, such as an SE, cooperating with the client device, or a remote device, such as a remote server. The hardware component may be incorporated within or connected or coupled to the

client device, a local device, such as an SE, cooperating with the client device, or a remote device, such as a remote server.

It is noteworthy that the hash distance generation step provides a hash distance that allows to determine whether the generated hash is more or less close to a predefined reference hash. The hash distance allows inferring whether the corresponding captured context data element(s) is(are) or is(are) not successfully authenticated, i.e. sufficiently close to respective predetermined reference captured context data element(s).

The hash distance may be generated through a hash type comparison algorithm.

An authentication of the concerned (local) environment or context under survey is therefore carried out through such a hash distance that is specific to (or characterizes) the invention solution.

The hash distance allows the invention solution to be resilient to more or less small changes with respect to the predefined reference hash while still authenticating successfully the concerned (local) environment or context, i.e. the value of at least some captured (or collected) context data element(s) has changed slightly.

It is to be noted that the hash or digest, as a byte stream relating to original captured context data element(s), is a string of bits with a resulting length, from e.g. 32 bytes to e.g. a few kbytes. The resulting length may be (or not) variable according to the captured context data element(s).

The hash relates to the original (captured) context data element(s) and reduces the number of bits (or elements of information) to be transferred with respect to the original context data element(s).

Contrary to the aforementioned prior art solution, the invention solution does not need a large bandwidth to transmit data, including the hash, relating to the concerned environment or context, since the data relating to the concerned context includes only a few data (up to a few kbytes) to be transmitted.

Contrary to the aforementioned prior art solution, the invention solution is therefore efficient.

Moreover, the hash obfuscates the concerned original context data element(s), i.e. does not disclose any original context data element(s) in plain text.

Since no data relating to the privacy is transmitted in plain text, the invention is thus compliant with data privacy and therefore the Generation Data Protection Regulation (or GDPR).

Contrary to the aforementioned prior art solution, due to the use of a hash (and not the use of the concerned captured context data element(s) in plain text), the invention solution is secure.

The invention solution is an environment or context authentication solution that allows authenticating the concerned (local) environment or context under survey.

The invention solution is user convenient.

Advantageously, the predetermined hash type algorithm comprising a Locality Sensitive Hash (or LSH) type algorithm, the method further comprises, as the hash distance generation step and the authentication step, the following steps:

- generating, by using the locality sensitive hash type algorithm, a score, as a level of similarity between the generated hash and the predetermined reference hash;
- comparing the score to a predetermined threshold value;
- authenticating successfully only if the score is equal to or greater than the predetermined threshold value.

The LSH type algorithm, as a hash type algorithm, is advantageously used to generate a score, as a hash distance used for comparing the generated hash to the predefined reference hash.

The generated score is then checked with respect to a predefined threshold value, so as to authenticate (or not) the concerned context.

Thus, the invention solution may be, through the score, as the hash distance, more or less permissive with respect to the predefined reference hash that has to be approached by the generated hash from the collected context data element(s).

It is to be noted that the score is either the hash distance itself or the result of a computation derived from the (hash) distance depending on the used algorithm for comparing the generated hash.

According to an additional aspect, the invention is a first authentication device.

According to the invention, the first authentication device is configured to:

- collect, based on a predetermined authentication policy, at least one context data element;
- constitute, based on the at least one collected context data element, a data packet;

- generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash; and
- send to a second device the generated hash.

The first authentication device may be a mobile phone, a PC or any computing device.

According to an additional aspect, the invention is a second authentication device.

According to the invention, the second authentication device is configured to:

- receive a generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

The second authentication device may be a secure element, a remote server or any computing device.

According to still a further aspect, the invention is an authentication system.

According to the invention, the system comprising a first authentication device and at least one second authentication device, the first authentication device is configured to:

- collect, based on a predetermined authentication policy, at least one context data element;
- constitute, based on the at least one collected context data element, a data packet;
- generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- send to the second authentication device, the generated hash; and

the second authentication device is configured to:

- receive from the first device, the generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

Brief description of the drawings:

Additional features and advantages of the invention will be apparent from a detailed description of one preferred embodiment of the invention, given as an indicative and non-limitative example, in conjunction with the following drawings:

- Figure 1 illustrates a simplified diagram of an exemplary embodiment of a system comprising a mobile phone and a server, the phone being configured to collect, based on a predefined authentication policy, a data element(s) comprised within the phone context, constitute a corresponding data packet, generate a corresponding hash, and send to the server the hash, the server being configured to generate a hash distance between the hash and a predetermined reference hash and authenticate, based on to the hash distance, the concerned context, according to the invention; and
- Figure 2 represents an example of a flow of messages exchanged between the user, the phone and the server of the system of figure 1, so that the server receives a hash generated at the client side, generates a corresponding hash distance and authenticates (or not), thanks to the generated hash distance, the concerned context.

Detailed description:

Herein under is considered an exemplary embodiment in which the invention authentication method is implemented notably by a phone, as a client (computer) device and a standalone entity, i.e. without cooperating with another device, such as an SE, and a remote server.

According to another exemplary embodiment (not represented), the invention authentication method is implemented by a computer device, as a terminal, in cooperation with an SE embedded within or connected to the terminal. According to such an embodiment, the SE, as a local and second authentication device, is adapted to perform the functions that are carried out by the server and described herein below while enhancing the security of stored and/or processed data.

The SE may be an incorporated chip, as a chip soldered, possibly in a removable manner, like e.g., an embedded SE, an embedded Universal Integrated Circuit Card (or eUICC) or an integrated Universal Integrated Circuit Card (or iUICC), on a Printed Circuit Board (or PCB) of the terminal, or a chip that is coupled to the terminal and included within a Universal Serial Bus (or USB), a smart card or any other medium (that may have different form factors), as an SE host device. The chip may thus be fixed to or removable from its host device, like e.g., the mobile phone.

The invention does not impose any constraint as to a kind of the SE type.

Naturally, the herein below described embodiment is only for exemplifying purposes and is not considered to reduce the scope of the present invention.

Figure 1 shows schematically an (authentication) system 10 that includes a (mobile) phone 14 and a remote (web) server 16.

The system is arranged to authenticate (or not) a context 12 (or environment) under survey.

The context 12 includes e.g. a user 11, as the owner of the phone 14.

Additionally (or alternately), the context 12 includes e.g. a TeleVision (or TV) set 13, as a physical object or thing.

However, the invention (authentication) solution is also applicable when the context 12 includes one or several human beings (and/or animal(s)) and/or one or several (physical) things.

For the sake of simplicity, only one phone 14, as a first (authentication) device, and only one user 11 and one object, as context data elements, have been represented.

However, the server 16, as a second (authentication) device, manages a set of context accounts and respective reference (context) hashes that have been previously respectively registered while using the same invention authentication process.

Instead of being constituted by a phone, the first device may be constituted by e.g., a smart phone, a PC, a vehicle, a virtual reality device, an augmented reality device, an Internet Of Things type device, a set-top box, a tablet computer, a desktop computer, a laptop computer, a video player, an audio player, a media-player, a game console, a netbook, a Personal Digital Assistant (or PDA), and/or any other computer device. Such a list of first devices is given as mere examples for a first device that may be used without being exhaustive.

Instead of being constituted by a physical first device, a software component, such as a library, or a hardware component carries out the functions that are described infra and that are performed by the phone 14.

The phone 14 includes one or several Central Processing Unit(s) (or CPU), (micro)processor(s) and/or (micro)controller(s) (not represented), as data processing means, one or several memories (not represented), as data storing means, and one or several Input/Output (or I/O) interfaces (not represented).

The (or each) phone processor processes data originating from and/or intended to any internal component and data originating from and/or intended to any external device through one or several phone I/O interfaces.

The phone memories may include one or several EEPROMs (acronym for "Electrically Erasable Programmable Read-Only Memory"), one or several ROMs (acronym for "Read Only Memory"), one or several Flash memories and/or any other memories of different types, like e.g., one or several RAMs (acronym for "Random Access Memory").

The phone 14 supports one or several Operating Systems (or OS).

The phone 14 supports a client application that allows the phone 14 to send, after a context data element collection, a corresponding data packet constitution and a corresponding hash generation, to the server 16 information including the generated hash. The generated hash allows the server 16 to authenticate (or not) the concerned context 12.

A phone 14 memory (and/or a memory of another device connected or coupled to the phone 14) stores a Mobile Station International Subscriber Directory Number (or MSISDN), as the phone 14 number, and/or the like, as a phone 14 Identifiers (or ID), , an International Mobile Equipment Identity (or IMEI), an email address and/or other data that allow(s) uniquely identifying the phone 14, as the first device.

The phone I/O interface(s) may comprise (and/or be connected to) a display screen and a keyboard, as a phone Man Machine Interface (or MMI), so as to interact with the user 11.

The phone I/O interface(s) includes e.g., a camera 142, so as to capture or collect video or picture data that is included in the environment or context that is present in front of the camera 142.

The phone I/O interface(s) includes e.g., one or several sensors that allow each to collect data relating to the context of the phone 14.

The phone I/O interface(s) includes e.g., an antenna 144, allowing to transmit data, through a Radio-Frequency (or RF) link(s) 15, as a wireless link(s), via a possible (communication) network(s), to the server 16.

The RF may be fixed at several hundreds of MHz, e.g., around 850, 900, 1800, 1900 and/or 2100 MHz, as Long Range (or LR) type RF.

The RF link 15 between the phone 14 and the server 16 is at least mono-directional, namely at least an uplink, i.e. from the phone 14 to the server 16.

The channel may be related to an HyperText Transfer Protocol (or HTTP) (Secure) (registered trademark) type channel, an Over-The-Air (or OTA), an Over-The-Internet (or OTI) type channel or any other data communication channel.

The channel using the RF link 15 may be secure or unsecure.

The phone 14 is arranged to collect, based on a predetermined authentication policy, an image (or picture) (and/or a video signal) including image data relating to the user 11 face and image data relating to the TV 13, as data elements included in the context (relating to the phone 14).

To collect a context data element(s), the phone 14 may use a Machine Learning (or ML) engine to analyse a collected (or captured) image.

Each context data element is preferably a string of bits (or units of information) with an individual fixed length.

The authentication policy allows configuring the phone 14 to process data originating from a surrounding environment of the phone 14, so as to authenticate the concerned environment.

The authentication policy is preferably previously (prior to launching an authentication process) provided by the server 16 or another server (not represented) connected to the server 16. The authentication policy comprises a set of identified context data elements to be collected, so as to define context data element(s) to be collected.

As context data element(s), the context data element(s) may include, besides image data relating to the user face and image data relating to the TV 13, other data, such as a phone ID, a Service Set IDentifier (or SSID), an OS version ID, geolocation data (like e.g., Global Positioning System (or GPS) data), a user 11 heart rate (not represented) and/or other data. To collect a context data element(s), the phone 14 may get or retrieve data, such as a phone ID, stored in a memory included within the phone 14 or a device connected or coupled to the phone 14.

The authentication policy may also define how the concerned context data element(s) is transformed into a corresponding data packet, how the resulting data packet is possibly processed, such as grouped, ciphered, weighted and/or sorted, and/or how a corresponding hash has to be generated.

The authentication policy may comprise information allowing to group together at least certain collected context data elements with respect to the other collected context

data element(s). Thus, certain context data elements are to be grouped within one and the same group, such as data relating to the operation of the phone 14, like e.g., an SSID and/or an OS version ID, and/or data relating to the audio and/or visual environment.

When two or more collected context data elements are grouped, the concerned collected context data element group impacts the corresponding generated hash distance (or score) by increasing the hash distance (or score) variation, i.e. if at least one of the collected context data elements within a concerned group changes, then the resulting corresponding generated hash distance (or score) varies more than if all of the collected context data elements of the group were kept (individually) separated from each other.

The authentication policy may comprise data for requesting that a data packet that results from the context data element(s) (possibly grouped at least in part) has to be ciphered by using a key generated from submitted user authentication data (or one or several data items originating from one or several external sources, such as a thermometer) (instead of being ciphered, being processed by a keyed one way function (i.e. non reversible), such as HMAC type function). Such a data packet ciphering request may further specify to use a specific encryption key, a specific encryption key generation algorithm, a specific data encryption algorithm and/or a process to generate the concerned encryption key or algorithm. The encryption key may be generated by using user authentication data, such as a Personal Identity Number (or PIN), a One-Time Password (or OTP), a password and/or a biometric user feature(s), such as a one or several user fingerprints, a user iris, a user face and/or a user palm(s), and/or data provided by one or several external sources, such as an SE, as input to an (identified) key generation algorithm. The encryption key may be generated by using a Hash-based Message Authentication Code (or HMAC) key derivation function.

The authentication policy may comprise data for identifying a user authentication to be used for authenticating the user 11, when applicable, i.e. when the user authentication data is to be included in the context data element(s). For example, the user 11 has to authenticate by providing a PIN, an OTP, a password and/or a biometric user feature(s), such as a one or several user fingerprints, a user iris, a user face and/or a user palm(s).

The authentication policy may comprise one or several weights to be associated with a specific (identified) group(s) and/or a specific (identified) context data element(s), so as to give heavier importance to the concerned group(s) and/or context data element(s) with respect to the other collected group(s) and/or collected context data element(s) within a corresponding data packet.

The authentication policy may comprise data for requesting that, prior to generating a corresponding hash, the context data element(s) (possibly grouped at least in part) has to be sorted, according to a predetermined numerical order, such as an increasing or decreasing numerical order.

The authentication policy may comprise data for identifying a hash type algorithm to be used for generating a hash relating to the collected context data element(s).

The authentication policy may comprise data for identifying several hash type algorithms to be used for generating several hashes relating to the collected context data elements which may have separate natures of data elements. The corresponding hash distance (or score) to be generated is then averaged (or weighted) the hashes resulting from each hash type algorithms.

Optionally, the phone 14 is arranged, preferably according to the authentication policy, to group at least two collected context data elements within the collected context data elements within the data packet.

The phone 14 is adapted to constitute, based on the collected context data element(s), a (resulting) data packet by e.g. concatenating the collected context data element(s).

The data packet is a kind of passphrase comprising, as word(s), the collected context data element(s).

The data packet is a string of bits (or units of information) with a resulting length that may vary depending on the collected context data element length(s) between separate context authentication sessions. The data packet length corresponds to an addition of all of the individual length(s) relating to the collected context data element(s).

Optionally, the phone 14 is adapted, preferably according to the authentication policy, to cipher or encrypt the data packet. Each of the context data elements that are possibly grouped at least in part is thus ciphered by using a predetermined encryption key. The encryption key may have been generated by using a HMAC type derivation function.

Optionally, the phone is adapted to weigh, according to the authentication policy, one or several (identified) collected context data element(s) of the collected context data element(s) that may have been previously grouped within the data packet. Such a collected context data element weighing may depend on a predetermined hash type algorithm to be used for generating a hash. Such a collected context data element weighing allows favouring the concerned collected context data element(s) and/or the concerned context data group(s) with respect to the other context data elements comprised within the concerned data packet. To weigh the concerned context data element(s), the phone 14 may duplicate the concerned context data element(s).

Optionally, the phone is arranged preferably according to the authentication policy, to sort, according to a numerical order, such as an increasing or a decreasing numerical order, the collected context data element(s) within the data packet. Such a (collected) context data element sorting allows preserving, depending on the used hash type algorithm, a generation of a corresponding hash and therefore a corresponding hash distance, i.e. the hash to be generated does not change when the concerned context data element sorting order is kept.

According to an essential invention feature, the phone 14 is configured to generate a hash by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm.

The predetermined hash type algorithm may be one of the following algorithms: a Locality Sensitive Hash (or LSH) type algorithm, a fuzzy matching type algorithm, a Trend micro Locality Sensitive Hash (or TLSH) type algorithm, a nilsimsa type algorithm, an sdhash type algorithm, an ssdeep type algorithm, an approximate matching type algorithm, a near duplicate matching type algorithm and a similarity detection type algorithm.

Such a list of hash type algorithms is given without being exhaustive as mere examples for an hash type algorithm that may be used for generating a hash with, as input, a data packet.

The hash type algorithm may incorporate a weighting, within the collected context data element(s), of one or several context data elements and/or one or several context data element group(s).

The phone 14 is arranged to send to the server 16, as a second (authentication) device, the generated hash.

Such a generated hash, as a cipher and a kind of context signature, allows not to disclose any original (user) private data that has been locally collected and therefore preserve the data privacy.

The generated hash has a fixed length that is a few data (up to a few kbits).

Instead of being constituted by a (physical) server, the second device may be constituted by e.g., a smart phone, a PC, a vehicle, a virtual reality device, an augmented reality device, an Internet Of Things type device, a set-top box, a tablet computer, a desktop computer, a laptop computer, a video player, an audio player, a media-player, a game console, a netbook, a Personal Digital Assistant (or PDA), and/or any other computer device. Such a list of second devices is given as mere examples for a second device that may be used without being exhaustive.

Instead of being constituted by a physical second device, a software component, such as a library, or a hardware component carries out the functions that are described infra and that are performed by the server 16.

The server 16 is connected to the phone 14 over the link 15.

The server 16 is remote and accessible through possibly one, two or more communication networks, such as an Intranet network and/or an Internet network, that allow to define or form a corresponding communication channel.

The corresponding communication channel may be secure or unsecure.

According to an alternative embodiment (not represented), the server 16 is local. For example, the server 16 is embedded within a device, such as an SE that is connected or coupled to the PC 14.

The server 16 may be operated or managed by a Mobile Network Operator (or MNO), a Mobile Virtual Network Operator (or MVNO), a banking Operator, a wire communication network operator, a service Operator (or administrator) or on behalf of a service Operator, as a service provider.

The server 16 includes one or several CPU(s), (micro)processor(s) and/or (micro)controller(s) 162, as data processing means, one or several memories 164, as data storing means, and one or several I/O interfaces 166 that are internally together connected.

A (or the) server I/O interface 166 is used for communicating with external devices, such as the first device 14.

A (or the) server memory 164 stores preferably, besides an OS, an invention (server) authentication application accessible from the server 16 processor.

A (or the) server memory 164 stores or registers a database.

The database includes a set of e.g. first device accounts. The database relates to a set of e.g. first devices, as a fleet of first devices.

Each first device account may include one or several associated user identifiers, such as a user name.

The database includes preferably, in association with e.g. each (identified) first device account, a corresponding predetermined reference hash.

The predetermined reference hash has been previously (i.e. during an enrolment or registration phase and prior to any (context) authentication) registered while using the invention authentication process.

The database may associate, for each individual first device or the first device set, a registered predetermined hash type algorithm.

The predetermined hash type algorithm may be one of the following algorithms an LSH type algorithm, a fuzzy matching type algorithm, a TLSH type algorithm, a nilsimsa type algorithm, an sdhash type algorithm, an ssdeep type algorithm, an approximate matching type algorithm, a near duplicate matching type algorithm and a similarity detection type algorithm.

Such a list of hash type algorithms is given without being exhaustive as mere examples for an hash type algorithm that may be used for generating a hash distance with, as inputs, a generated hash (to be received from a client device) and a corresponding (registered) reference hash.

The database may associate, for each individual first device or the first device set, a registered predetermined threshold value.

The predetermined threshold value has been previously (i.e. prior to any (context) authentication) registered. The predetermined threshold value is configurable according to a level of risk that the concerned service provider may take.

The (or each) server processor processes data originating from and/or intended to any internal component and data originating from and/or intended to any external device through one or several server I/O interfaces.

The server 16 supports one or several OSs.

The server 16 supports a server application that allows the server 16, after a hash reception and a corresponding hash distance generation, to authenticate (or not), based on the hash distance, the concerned phone context.

The server 16 may be configured to generate and send an authentication policy to the first device, such as the phone 14, prior to any first device enrolment.

The server 16 is adapted to receive, from an (identified) client device, such as the phone 14, a generated hash.

The server 16 identifies, based on a received e.g. client device ID(s), a corresponding first device registered within the database accessible to the server 16.

Then, the server 16 retrieves a predetermined reference hash that is registered in association with the registered first device or a corresponding first device fleet.

According to an essential invention feature, the server 16 is configured to generate on-the-fly, i.e. when a first device launches a login (or connection) session with the server 16, a score, as a hash distance between the (received) generated hash and a (registered) predetermined reference hash.

To generate the score, the server 16 uses the (retrieved) predetermined hash type algorithm and the (retrieved) predetermined reference hash.

The server 16 is adapted to authenticate successfully or not, based on the generated hash distance, the concerned context 12.

More exactly, the server 16 is configured to fail to authenticate the context 12 if the generated hash distance is less than the (retrieved) predetermined threshold value.

The server 16 is configured to succeed in authenticating the context 12 if the generated hash distance is equal to or greater than the (retrieved) predetermined threshold value.

The server 16 may be adapted to store, preferably in a secure and persistent manner, the (received) generated hash, each time the authentication is successful. Such a generated hash storage when the authentication is successful allows to trace the success authentication history or evolvement.

Alternately (or additionally), each time the authentication is successful, the server 16 is arranged to register, instead of the predetermined reference hash, the (received) generated hash, as an updated reference hash to be used for a next authentication. The authentication process taking into account the last generated hash, as the updated

reference hash for a new (context) authentication, lets evolve the corresponding reference hash with the time at each authentication success.

Figure 2 depicts an example of a message flow 20 that involves the phone 14 and the server 16, so that the server 16 authenticates the context 12 based on a hash distance between a (received) generated hash and a (registered) predetermined reference hash.

It is assumed that the authentication policy has been provided during a personalization phase to the phone 14. The authentication policy requests to collect an image relating to the user 11 face, an image relating to the TV 13 and a phone ID, as three context data elements to be detected, so as to authenticate the user 11.

It is further assumed that the server 16 has previously registered (not represented) a user 11 ID in association with the phone 14 number, as a phone ID, a predetermined reference hash corresponding to the user 11 face image, the TV 13 image and the phone ID, as corresponding context data elements, a predetermined threshold value, such as e.g. 75%, and a predetermined hash type algorithm to be used for generating a hash distance.

It is assumed that the predetermined hash type algorithm to be used for generating a hash and a corresponding hash distance is e.g. a LSH type algorithm.

The use of an LSH type algorithm allows generating similar hashes, i.e. a hash distance or score that is good, i.e. the score is equal or greater than the predefined threshold value, when there is a slight change between the hash relating to the current context under survey and the reference hash relating to a corresponding reference context.

The phone 14 thus constitutes a reference first (communication) device to be locally present within the user 11 context 12, so as to authenticate, through the context 12, the user 11.

It is further assumed that the phone 14 accesses the phone 14 ID and an image signal captured by the phone camera 142.

An execution of the client application supported by the phone 14 is automatically launched (i.e. without any involvement of the user 11).

Alternately, the user 11 launches the client application while using an MMI that is included in or connected to the phone 14.

The phone 14 gets, through the phone camera 142, an image signal 22 relating to all the physical human(s) (and/or animal(s)) and/or thing(s) that are present in front of the phone 14.

In the present scenario, the image signal includes e.g. the user 11 face image and the TV 13 image.

The phone 14 retrieves (not represented) from a phone memory the MSISDN of the phone 14, as the phone 14 ID.

Instead of collecting the phone 14 ID from a phone memory, the phone 14 collects from a locally connected device, such as an SE that has preferably authenticate a user e.g. through a PIN comparison to a reference PIN that is stored in an SE memory, the phone 14 ID 23.

The phone 14 collects 24 the user 11 face image and the TV 13 image while extracting from the image signal 22 the user 11 face image and the TV 13 image and the phone 14 ID, as three context data elements required by the authentication policy.

The phone 14 may group 26, based on the authentication policy, at least two context data elements, e.g., the user 11 face image and the TV 13 image, as one and the same context data element group, within the collected data elements.

The phone 14 constitutes 28, based on the collected context data elements, a data packet by e.g. concatenating the collected context data elements

Optionally, the phone 14 enciphers 210, based on the authentication policy, the (resulting) data packet, so as to improve the security aspect. The data packet that is thus enciphered while using a key depending on e.g. user authentication impacts on the corresponding hash distance (or score). If the user is not successfully authenticated (at the client side), then the corresponding resulting hash is remote from a predetermined reference hash leading to a "bad" hash distance (or score) and therefore a failure of context authentication (even if the other collected context data element(s) is(are) right with respect to a collected reference context data element(s) that produces the corresponding predetermined reference hash).

The phone 14 may weigh 212, based on the authentication policy (or the used predetermined hash type algorithm), more or less heavy, one or several collected context data elements and/or one or several groups of collected context data elements with respect to the other collected context data elements within the data packet.

Optionally, the phone 14 sorts 214, according to a numerical order, such as a decreasing or an increasing order, the collected context data elements that are possibly grouped at least in part, possibly enciphered and/or possibly weighted, within the data packet.

Then, the phone 14 generates 216, by using e.g. a nilsimsa algorithm and the data packet, as input to the nilsimsa algorithm, a hash.

The phone 14 sends, through e.g., a Short Message Service (or SMS), Multimedia Messaging Service (or MMS), Transmission Control Protocol/Internet Protocol (or TCP/IP), or HTTP(s) type channel, to an (identified) server 16 a message 218 that includes the phone ID and the generated hash.

Once the server 16 has received the message, the server 16 identifies (not represented), based on the phone ID, the concerned user 11 account and thus the associated predetermined reference hash and the associated predetermined hash type algorithm to be used for generating a hash distance.

Then, the server 16 generates a hash distance between the (received) generated hash and the predetermined reference hash.

To generate the hash distance, the server 16 gets the reference hash and generates 220 a score by using e.g. the nilsimsa algorithm and the received generated hash and the predetermined reference hash, as the two inputs to the nilsimsa algorithm. The score is considered as a level of similarity between the received generated hash and the predetermined reference hash. For instance with the nilsimsa algorithm, the score is "0" (zero) when there is no similarity i.e.0% of similarity, is "96" when there is 75% of similarity and is "128" when there is a full similarity, i.e. 100% of similarity.

Once the server 16 has generated the hash distance, the server 16 verifies 222 whether the authentication is or is not successful based on the generated hash distance. To do such an authentication verification, the server 16 compares 222 the generated score with respect to the predetermined threshold value.

If the generated score is less than the predetermined threshold value, then the server 16 fails 223 to authenticate, through the user context 12, the user 11 and denies user access to the service(s) managed by or through the server 16.

Otherwise, i.e. if the generated score is equal to or greater than the predetermined threshold value, then the server 16 succeeds 224 in authenticating, through the user

context 12, the user 11 and grants user access to a service(s) managed by or through the server 16.

Optionally, if the generated score is equal to or greater than the predetermined threshold value, the server 16 registers 226 the received generated hash by either further enriching (or adding to) a database relating to the reference hashes in case of authentication success or substituting the received generated hash to the registered predetermined reference hash. Thus, in this latter case, the authentication process is continuously adaptive along the way the authentication context is evolving.

Optionally, the server 16 sends (not represented) to the phone 14, through the same channel or an out-of-band channel than the one used for the submission of the generated hash, a message that includes a request to present or display the authentication result. Then, the phone 14 presents or displays the authentication result (not represented), such as “authentication failure” or “authentication success”.

For the user, the invention solution is simple, easy, quick and practical since the user does not need to be involved. As a matter of fact, the user has just to present her or his face and the TV in front of the camera. The user does not need to enter any data, like e.g., an OTP, a number or a text on the first device, so as to let a first part collect the required context data elements and issue a corresponding hash to be verified by a second part, as its addressee, in order to be authenticated.

The invention solution allows carrying out a secure and efficient context authentication based on a hash distance that allows keeping flexibility.

The invention solution allows adapting to more or less small authentication context data element change(s), according to a level of risk to be adopted.

The invention solution does not include any oracle on the client (device) since it has no means for validating or verifying the generated hash. As a matter of fact, only the server is able to verify the generated hash.

The invention solution prevents thus from a client side brute-force attack of user authentication.

The embodiment that has just been described is not intended to limit the scope of the concerned invention. Other embodiments may be given. As another embodiment, instead of using an LR RF technology channel to transmit information to the second device, the first device uses a Short Range (or SR) RF technology(ies), like e.g., a Wi-

Fi, Bluetooth, a Near Field Communication or a Bluetooth Low Energy type technology(ies).

CLAIMS

1. An authentication method (20) comprising:

- collecting (24), based on a predetermined authentication policy, at least one context data element;
- constituting (28), based on the at least one collected context data element, a data packet;
- generating (216), by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- sending the generated hash;
- generating (220), as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and
- authenticating (224) successfully or not (223) based on the generated hash distance, as an authentication step.

2. Method according to claim 1, wherein, the predetermined hash type algorithm comprising a locality sensitive hash type algorithm, the method further comprises, as the hash distance generation step and the authentication step, the following steps:

- generating, by using the locality sensitive hash type algorithm, a score, as a level of similarity between the generated hash and the predetermined reference hash;
- comparing the score to a predetermined threshold value;
- authenticating successfully only if the score is equal to or greater than the predetermined threshold value.

3. Method according to claim 1 or 2, wherein, prior to generating the hash, the method further comprises sorting, according to a numerical order, the at least one collected context data element within the data packet.

4. Method according to any previous claim, wherein, prior to generating the hash, the method further comprises weighting, according to the authentication policy, at least one of the at least one context data element.

5. Method according to any previous claim, wherein, prior to constituting the data packet, the method further comprises grouping, according to the authentication policy,

together at least two context data elements comprised within the at least one context data element, to constitute at least one corresponding context data group.

6. Method according to any previous claim, wherein, prior to generating the hash, the method further comprises ciphering, according to the authentication policy, the data packet.

7. Method according to claim 6, wherein a key used for the data packet ciphering includes a key generated by using a hash-based message authentication code key type derivation function.

8. Method according to any previous claim, wherein the hash type algorithm includes at least one element of a group including:
- a locality sensitive hash type algorithm;
- a Trend micro Locality Sensitive Hash type algorithm;
- a nilsimsa type algorithm;
- an sdhash type algorithm;
- an ssdeep type algorithm; and
- a fuzzy matching type algorithm;
- an approximate matching type algorithm;
- a near duplicate matching type algorithm; and
- a similarity detection type algorithm.

9. Method according to any previous claim, wherein, each time the authentication is successful, the method further comprises storing the generated hash.

10. Method according to any previous claim, wherein, each time the authentication is successful, the method further comprises registering, instead of the predetermined reference hash, the generated hash, as an updated reference hash to be used for a next authentication.

11. A first authentication device (14), **characterized in that** the first authentication device is configured to:

- collect, based on a predetermined authentication policy, at least one context data element;
- constitute, based on the at least one collected context data element, a data packet;
- generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash; and
- send to a second authentication device the generated hash.

12. Device according to claim 11, wherein the first authentication device includes includes at least one element of a group including:
- a mobile phone;
- a Personal Computer;
- a vehicle;
- a desktop;
- a virtual reality device;
- an augment reality device;
- an Internet Of Things type device; and
- a computing device.

13. A second authentication device (16), **characterized in that** the second authentication device is configured to:
- receive a generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

14. Device according to claim 13, wherein the second authentication device includes at least one element of a group including:
- a secure element;
- a local server;
- a remote server;
- a mobile phone;
- a Personal Computer;
- a vehicle;

- a desktop;
- a virtual reality device;
- an augment reality device;
- an Internet Of Things type device;
- a computing device.

15. An authentication system (10), **characterized in that,** the system comprising a first authentication device (14) and at least one second authentication device (16), the first authentication device is configured to:

- collect, based on a predetermined authentication policy, at least one context data element;
- constitute, based on the at least one collected context data element, a data packet;
- generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- send to the second authentication device, the generated hash; and

in that the second authentication device is configured to:

- receive from the first device, the generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

AUTHENTICATION METHOD, DEVICE AND SYSTEM

ABSTRACT

The invention relates to an authentication method. The method comprises:

- collecting 24, based on a predetermined authentication policy, at least one context data element;
- constituting 28, based on the at least one collected context data element, a data packet;
- generating 216, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- sending the generated hash;
- generating 220, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and
- authenticating 224 successfully or not 223 based on the generated hash distance, as an authentication step.

The invention also relates to corresponding device and system.

Figure 2

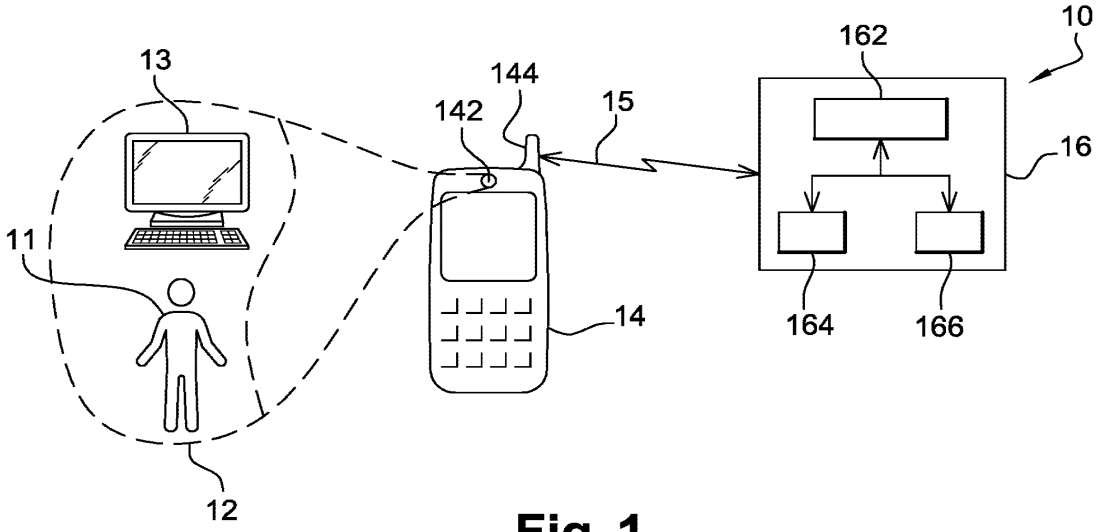


Fig. 1

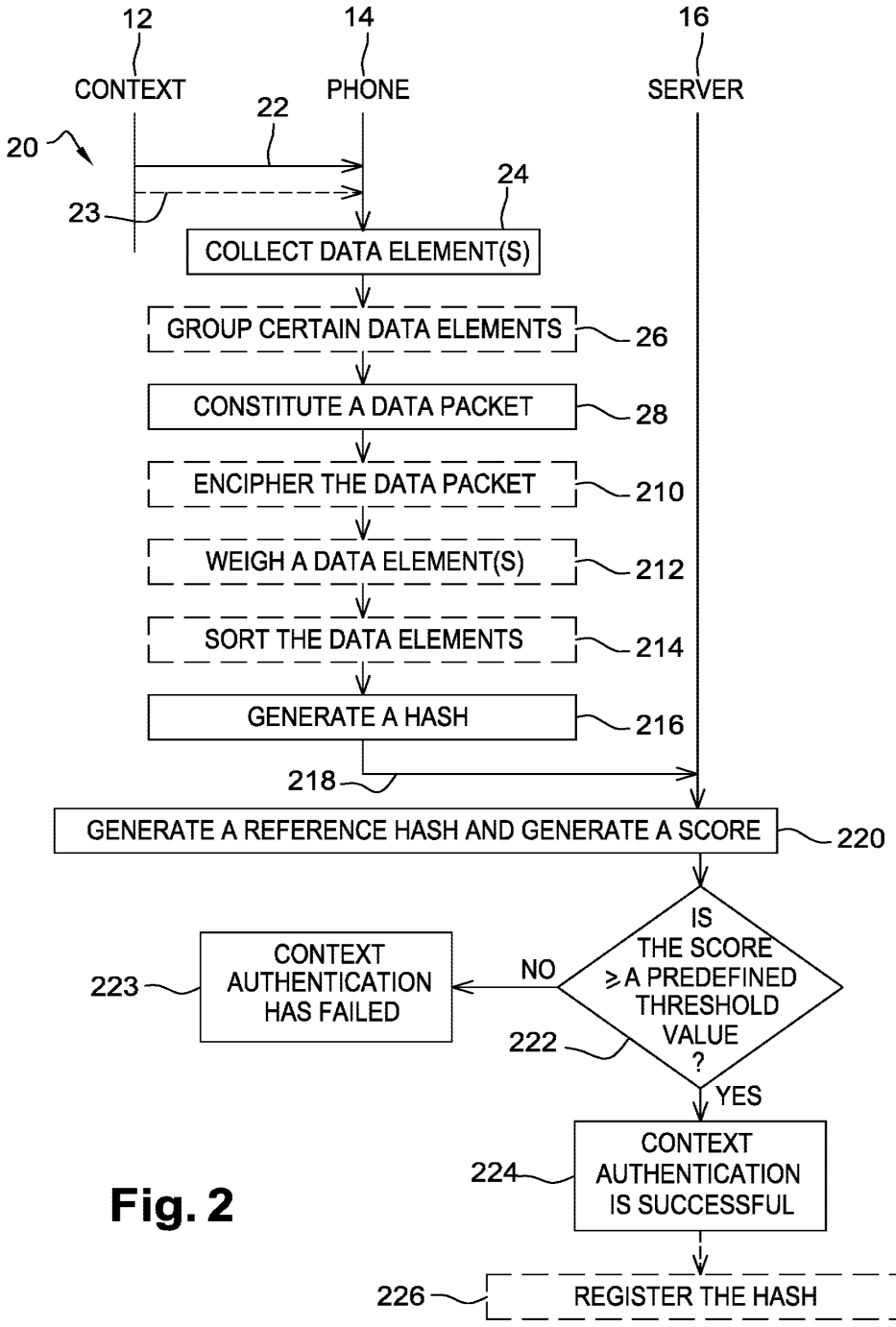

12
CONTEXT
14
PHONE
16
SERVER
20
22
23
24
COLLECT DATA ELEMENT(S)
GROUP CERTAIN DATA ELEMENTS
26
CONSTITUTE A DATA PACKET
28
ENCIPHER THE DATA PACKET
210
WEIGH A DATA ELEMENT(S)
212
SORT THE DATA ELEMENTS
214
GENERATE A HASH
216
218
GENERATE A REFERENCE HASH AND GENERATE A SCORE
220
IS THE SCORE ≥ A PREDEFINED THRESHOLD VALUE ?
222
NO
223
CONTEXT AUTHENTICATION HAS FAILED
YES
224
CONTEXT AUTHENTICATION IS SUCCESSFUL
226
REGISTER THE HASH

Fig. 2

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF RECEIPT OF RECORD COPY

(PCT Rule 24.2(a))

To:

SCHEER, Luc
525 avenue du Pic de Bertagne CS 12023
13881 Gemenos Cedex
FRANCE

Date of mailing *(day/month/year)*	IMPORTANT NOTIFICATION
27 November 2018 (27.11.2018)	
Applicant's or agent's file reference	International application No.
GMT3707WO/DD	PCT/EP2018/081759

The applicant is hereby **notified** that the International Bureau has received the record copy of the international application as detailed below.

Name(s) of the applicant(s) and State(s) for which they are applicants:

GEMALTO SA (all designated States)

International filing date: 19 November 2018 (19.11.2018)
Priority date(s) claimed: 29 December 2017 (29.12.2017)
Date of receipt of the record copy by the International Bureau: 22 November 2018 (22.11.2018)
List of designated Offices:

AP: BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW
EA: AM, AZ, BY, KG, KZ, RU, TJ, TM
EP: AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR
OA: BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG
National: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW

ATTENTION: The applicant should carefully check the data appearing in this Notification. In case of any discrepancy between these data and the indications in the international application, the applicant should immediately inform the International Bureau. **In addition, the applicant's attention is drawn to:**

- time limits for entry into the national phase (see www.wipo.int/pct/en/texts/time_limits.html and *PCT Applicant's Guide*, National Phase, especially Chapters 3 and 4)
- requirements regarding priority documents (if applicable) (see *PCT Applicant's Guide*, International Phase, paragraph 5.070)

A copy of this notification is being sent to the receiving Office and to the International Searching Authority.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 70 80

Authorized officer
Ulhaq Faizan
e-mail pct.team3@wipo.int
Telephone No. +41 22 338 74 05

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING SUBMISSION, OBTENTION OR TRANSMITTAL OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

To:

SCHEER, Luc
525 avenue du Pic de Bertagne CS 12023
13881 Gemenos Cedex
FRANCE

Date of mailing *(day/month/year)* 04 December 2018 (04.12.2018)	
Applicant's or agent's file reference GMT3707WO/DD	IMPORTANT NOTIFICATION
International application No. PCT/EP2018/081759	International filing date *(day/month/year)* 19 November 2018 (19.11.2018)
International publication date *(day/month/year)* **Not yet published**	Priority date *(day/month/year)* 29 December 2017 (29.12.2017)
Applicant GEMALTO SA	

The applicant is hereby notified of the date of receipt (or of obtaining by the International Bureau) of the priority document(s) relating to all earlier application(s) whose priority is claimed. Unless otherwise indicated by the letters "NR", in the right-hand column or by an asterisk appearing next to the date of receipt, **the priority document concerned was submitted or transmitted to or obtained by the International Bureau in compliance with Rule 17.1(a), (b) or (b-*bis*)**. This Form replaces any previously issued notification concerning submission, transmittal or obtaining of priority documents.

Priority date	Priority application No.	Country or regional Office or PCT receiving Office	Date of receipt of priority document
29 December 2017 (29.12.2017)	17306977.4	EP	28 November 2018 (28.11.2018)

The letters "NR" denote a priority document which, on the date of mailing of this Form, had not yet been received or obtained by the International Bureau in compliance with Rule 17.1(a), (b) or (b-*bis*). Where the applicant has failed to either submit, request to prepare and transmit, or to request the International Bureau to obtain the priority document within the applicable time limit under that Rule, the attention of the applicant is directed to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

An asterisk "*" next to a date of receipt, denotes a priority document submitted or transmitted to or obtained by the International Bureau but not in compliance with Rule 17.1(a), (b) or (b-*bis*) (the priority document was received after the time limit prescribed in Rule 17.1(a); the request to prepare and transmit the priority document was submitted to the receiving Office after the applicable time limit under Rule 17.1(b) or the request to the International Bureau to obtain the priority document was made after the applicable time limit under Rule 17.1(b-*bis*)). Even though the priority document was not furnished in compliance with Rule 17.1(a), (b) or (b-*bis*), the International Bureau will nevertheless transmit a copy of the document to the designated Offices, for their consideration. In case such a copy is not accepted by the designated Office as the priority document, Rule 17.1(c) provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 70 80

Authorized officer
Nora Lindner
e-mail pct.team5@wipo.int
Telephone No. +41 22 338 74 05

Thales Exhibit 2001, Page 297 of 339
Okta v. Thales DIS France - IPR2026-00278

Expéditeur : le BUREAU INTERNATIONAL

PCT

NOTIFICATION DE L'ENREGISTREMENT D'UN CHANGEMENT

(règle 92*bis*.1 et instruction administrative 422 du PCT)

Destinataire :

SCHEER, Luc
525 avenue du Pic de Bertagne CS 12023
13881 Gemenos Cedex
FRANCE

Date d'expédition *(jour/mois/année)*
12 août 2019 (12.08.2019)

Référence du dossier du déposant ou du mandataire
GMT3707WO/DD

NOTIFICATION IMPORTANTE

Demande internationale n°
PCT/EP2018/081759

Date du dépôt international *(jour/mois/année)*
19 novembre 2018 (19.11.2018)

1. Les renseignements suivants étaient enregistrés en ce qui concerne :

☒ le déposant ☐ l'inventeur ☐ le mandataire ☐ le représentant commun

Nom et adresse
GEMALTO SA
6, rue de la Verrerie
92190 Meudon
FRANCE

Nationalité (nom de l'Etat) : FR
Domicile (nom de l'Etat) : FR
n° de téléphone :
n° de télécopieur :
Adresse électronique :

2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne :

☐ la personne ☐ le nom ☒ l'adresse ☐ la nationalité ☐ le domicile

Nom et adresse
THALES DIS FRANCE SA
6, rue de la Verrerie
92190 Meudon
FRANCE

Nationalité (nom de l'Etat) : FR
Domicile (nom de l'Etat) : FR
n° de téléphone :
n° de télécopieur :
Adresse électronique :
☐ Autorisation de recourir au courrier électronique

3. Observations complémentaires, le cas échéant :

4. Une copie de cette notification a été envoyée

☒ à l'office récepteur
☐ à l'administration chargée de la recherche internationale
☐ à l'[à l'] [aux] administration(s) indiquée(s) pour la recherche supplémentaire
☐ à l'administration chargée de l'examen préliminaire international
☒ aux offices désignés concernés
☐ aux offices élus concernés
☐ autre destinataire :

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

Fonctionnaire autorisé
Nissen Diana
e-mail diana.nissen@wipo.int
n° de téléphone +4122 338 8054

PATENT COOPERATION TREATY

WO 2019/129422
PCT/EP2018/081759

From the INTERNATIONAL BUREAU

PCT

SECOND AND SUPPLEMENTARY NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION (TO DESIGNATED OFFICES WHICH APPLY THE 30 MONTH TIME LIMIT UNDER ARTICLE 22(1))

(PCT Rule 47.1(c))

To:

SCHEER, Luc
525 avenue du Pic de Bertagne CS 12023
13881 Gemenos Cedex
FRANCE

Date of mailing *(day/month/year)*	
30 April 2020 (30.04.2020)	
Applicant's or agent's file reference	IMPORTANT NOTICE
GMT3707WO/DD	

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP2018/081759	19 November 2018 (19.11.2018)	29 December 2017 (29.12.2017)

Applicant

THALES DIS FRANCE SA

1. **ATTENTION**. For any designated Office(s), for which the time limit under Article 22(1), as in force from 1 April 2002 (30 months from the priority date), **does not apply**, please see Form PCT/IB/308(First Notice) issued previously.

2. Notice is hereby given that the following designated Office(s), for which the time limit under Article 22(1), as in force from 1 April 2002, **does apply**, has/have requested that the communication of the international application, as provided for in Article 20, be effected under Rule 93*bis*.1. The International Bureau has effected that communication on the date indicated below:
04 July 2019 (04.07.2019)

AZ, CN, EP, KG, KP, KR, MD, MK, MZ, NA, NG, PG, RU, TM

In accordance with Rule 47.1(*c-bis*)(i), those Offices will accept the present notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

3. The following designated Offices, for which the time limit under Article 22(1), as in force from 1 April 2002, **does apply**, have not requested, as at the time of mailing of the present notice, that the communication of the international application be effected under Rule 93*bis*.1 :

AE, AG, AL, AM, AO, AP, AT, AU, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EA, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KH, KN, KW, KZ, LA, LC, LK, LR, LS, LY, MA, ME, MG, MN, MW, MX, MY, NI, NO, NZ, OA, OM, PA, PE, PH, PL, PT, QA, RO, RS, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TN, TR, TT, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW

In accordance with Rule 47.1(*c-bis*)(ii), those Offices accept the present notice as conclusive evidence that the Contracting State for which that Office acts as a designated Office does not require the furnishing, under Article 22, by the applicant of a copy of the international application.

4. **TIME LIMITS for entry into the national phase**

For the designated or elected Office(s) listed above, the applicable time limit for entering the national phase will, **subject to what is said in the following paragraph,** be **30 MONTHS** from the priority date.

In practice, **time limits other than the 30-month time limit** will continue to apply, for various periods of time, in respect of certain of the designated or elected Office(s) listed above. For **regular updates on the applicable time limits** (30 or 31 months, or other time limit), Office by Office, refer to the *PCT Gazette*, the *PCT Newsletter* and the *PCT Applicant's Guide*, Volume II, National Chapters, all available from WIPO's Internet site, at http://www.wipo.int/pct/en/index.html.

It is the applicant's **sole responsibility** to monitor all these time limits.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 82 70

Authorized officer:

Nora Lindner

e-mail: pct.team3@wipo.int

Thales Exhibit 2001, Page 299 of 339
Okta v. Thales DIS France - IPR2026-00278

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING THE FILING OF AMENDMENTS OF THE CLAIMS

(PCT Administrative Instructions, Section 417)

To:

SCHEER, Luc
525 avenue du Pic de Bertagne CS 12023
13881 Gemenos Cedex
FRANCE

Date of mailing *(day/month/year)* 24 April 2019 (24.04.2019)	
Applicant's or agent's file reference GMT3707WO/DD	IMPORTANT NOTIFICATION
International application No PCT/EP2018/081759	International filing date *(day/month/year)* 19 November 2018 (19.11.2018)
Applicant GEMALTO SA	

1. The applicant is hereby notified that amendments to the claims under Article 19 were received by the International Bureau on:
19 April 2019 (19.04.2019) .

2. This date is
- ☒ within the time limit under Rule 46.1.
  Consequently, the international publication of the international application will contain the amended claims according to Rule 48.2(f), (h) and (i).
- ☐ after the expiration of the time limit under Rule 46.1.
  Consequently, the amendments will not be published and will not be considered for the international procedure.

3. The applicant is reminded that the international application (description, claims and drawings) may be amended during the international preliminary examination under Chapter II, according to Article 34, and in any case, before each of the designated Offices, according to Article 28 and Rule 52, or before each of the elected Offices, according to Article 41 and Rule 78.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Cabot Daniele e-mail pct.team5@wipo.int Telephone No. +41 22 338 74 05

gemalto
a Thales company

THALES

World Intellectual Property Organization
International Office

Gémenos, April 19th 2019

Ref.: GMT3707-WO/DD
Application: n° PCT/EP2018/081759
Applicant: GEMALTO SA

Subject: Amendment of the claims of the International Application

Dear Madam, dear Sir

Please find herewith attached a set of claims as amended under Article 19 PCT and Rule 46.1 PCT after the transmittal of the international search report and the written opinion of the international searching authority dated January 22nd 2019.

Claims 1-7 are unchanged.
Previous claims 8-10, 12 and 14 have been deleted.
Claims 8-10 are previous claims 11, 13 and 15 respectively.

With best regards.

David Dagès
Patent Engineer

Thales Exhibit 2001, Page 301 of 339
Okta v. Thales DIS France - IPR2026-00278

Claims

[Claim 1] An authentication method (20) comprising:

[Claim 2] collecting (24), based on a predetermined authentication policy, at least one context data element;

[Claim 3] constituting (28), based on the at least one collected context data element, a data packet;

[Claim 4] generating (216), by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;

[Claim 5] sending the generated hash;

[Claim 6] generating (220), as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and

[Claim 7] authenticating (224) successfully or not (223) based on the generated hash distance, as an authentication step.

[Claim 8] Method according to claim 1, wherein, the predetermined hash type algorithm comprising a locality sensitive hash type algorithm, the method further comprises, as the hash distance generation step and the authentication step, the following steps:
- generating, by using the locality sensitive hash type algorithm, a score, as a level of similarity between the generated hash and the predetermined reference hash;
- comparing the score to a predetermined threshold value;
- authenticating successfully only if the score is equal to or greater than the predetermined threshold value.

[Claim 9] Method according to claim 1 or 2, wherein, prior to generating the hash, the method further comprises sorting, according to a numerical order, the at least one collected context data element within the data packet.

[Claim 10] Method according to any previous claim, wherein, prior to generating the hash, the method further comprises weighting, according to the authentication policy, at least one of the at least one context data element.

[Claim 11] Method according to any previous claim, wherein, prior to constituting the data packet, the method further comprises grouping, according to the authentication policy, together at least two context data elements comprised within the at least one context data element, to constitute at least one corresponding context data group.

[Claim 12] Method according to any previous claim, wherein, prior to generating the hash, the method further comprises ciphering, according to the au-

thentication policy, the data packet.

[Claim 13] Method according to claim 6, wherein a key used for the data packet ciphering includes a key generated by using a hash-based message authentication code key type derivation function.

[Claim 14] A first authentication device (14), **characterized in that** the first authentication device is configured to:

[Claim 15] collect, based on a predetermined authentication policy, at least one context data element;

[Claim 16] constitute, based on the at least one collected context data element, a data packet;

[Claim 17] generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash; and

[Claim 18] send to a second authentication device the generated hash.

[Claim 19] A second authentication device (16), **characterized in that** the second authentication device is configured to:

- receive a generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

[Claim 20] An authentication system (10), **characterized in that,** the system comprising a first authentication device (14) and at least one second authentication device (16), the first authentication device is configured to:

[Claim 21] collect, based on a predetermined authentication policy, at least one context data element;

[Claim 22] constitute, based on the at least one collected context data element, a data packet;

[Claim 23] generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;

[Claim 24] send to the second authentication device, the generated hash; and **in that** the second authentication device is configured to:

[Claim 25] receive from the first device, the generated hash;

[Claim 26] generate a hash distance between the generated hash and a predetermined reference hash; and

[Claim 27] authenticate successfully or not based on the generated hash distance.

CLAIMS

1. An authentication method (20) comprising:

- collecting (24), based on a predetermined authentication policy, at least one context data element;
- constituting (28), based on the at least one collected context data element, a data packet;
- generating (216), by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- sending the generated hash;
- generating (220), as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and
- authenticating (224) successfully or not (223) based on the generated hash distance, as an authentication step.

2. Method according to claim 1, wherein, the predetermined hash type algorithm comprising a locality sensitive hash type algorithm, the method further comprises, as the hash distance generation step and the authentication step, the following steps:

- generating, by using the locality sensitive hash type algorithm, a score, as a level of similarity between the generated hash and the predetermined reference hash;
- comparing the score to a predetermined threshold value;
- authenticating successfully only if the score is equal to or greater than the predetermined threshold value.

3. Method according to claim 1 or 2, wherein, prior to generating the hash, the method further comprises sorting, according to a numerical order, the at least one collected context data element within the data packet.

4. Method according to any previous claim, wherein, prior to generating the hash, the method further comprises weighting, according to the authentication policy, at least one of the at least one context data element.

5. Method according to any previous claim, wherein, prior to constituting the data packet, the method further comprises grouping, according to the authentication policy,

together at least two context data elements comprised within the at least one context data element, to constitute at least one corresponding context data group.

6. Method according to any previous claim, wherein, prior to generating the hash, the method further comprises ciphering, according to the authentication policy, the data packet.

7. Method according to claim 6, wherein a key used for the data packet ciphering includes a key generated by using a hash-based message authentication code key type derivation function.

8. A first authentication device (14), **characterized in that** the first authentication device is configured to:
- collect, based on a predetermined authentication policy, at least one context data element;
- constitute, based on the at least one collected context data element, a data packet;
- generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash; and
- send to a second authentication device the generated hash.

9. A second authentication device (16), **characterized in that** the second authentication device is configured to:
- receive a generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

10. An authentication system (10), **characterized in that,** the system comprising a first authentication device (14) and at least one second authentication device (16), the first authentication device is configured to:
- collect, based on a predetermined authentication policy, at least one context data element;

- constitute, based on the at least one collected context data element, a data packet;
- generate, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash;
- send to the second authentication device, the generated hash; and

in that the second authentication device is configured to:

- receive from the first device, the generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	AUTHENTICATION METHOD, DEVICE AND SYSTEM
First Named Inventor/Applicant Name:	Fabrice DELHOSTE
Filer:	James A. LaBarre/Ashley Fernandez
Attorney Docket Number:	1032326-001016

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
NATIONAL STAGE FEE	1631	1	300	300
NATL STAGE SEARCH FEE - REPORT PROVIDED	1642	1	520	520
NATIONAL STAGE EXAM - ALL OTHER CASES	1633	1	760	760
Pages:				
Claims:				
INDEPENDENT CLAIMS IN EXCESS OF 3	1614	1	460	460
Miscellaneous-Filing:				
OATH/DECL > 30 MOS FROM 371 COMMENCEMENT	1617	1	140	140

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**2180**

Electronic Acknowledgement Receipt	
EFS ID:	39837474
Application Number:	16958252
International Application Number:	PCT/EP2018/081759
Confirmation Number:	5318
Title of Invention:	AUTHENTICATION METHOD, DEVICE AND SYSTEM
First Named Inventor/Applicant Name:	Fabrice DELHOSTE
Customer Number:	21839
Filer:	James A. LaBarre/Ashley Fernandez
Filer Authorized By:	James A. LaBarre
Attorney Docket Number:	1032326-001016
Receipt Date:	26-JUN-2020
Filing Date:	
Time Stamp:	12:13:18
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$2180
RAM confirmation Number	E20206PC13375607
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	APP_-_371_TL.pdf	974169 57d74ad089c60cb0af1fd68ea695b7251147a12a	no	4
Warnings:					
Information:					
2	Internet Communications Authorized	APP_-_Auth_for_Internet_Communication.pdf	607263 4ddaad7d842647f5f12e5ee07583ef19f6af6f9b	no	2
Warnings:					
Information:					
3	Authorization for Extension of Time all replies	APP_-_Gen_auth_of_fees.pdf	200590 0b94874435ba7a14f1044747d22fdbe1c60ef5375	no	1
Warnings:					
Information:					
4	Power of Attorney	APP_-_POA.pdf	1551507 ad4e48bc6b03b480ebcaa70e61fc7bd37dfe4909	no	2
Warnings:					
Information:					
5		PreliminaryAmendment.pdf	77085 3a96b041c59f7404ba9acffbd33d71c993ef9e95	yes	8

Multipart Description/PDF files in .zip description

Document Description	Start	End
Preliminary Amendment	1	1
Abstract	2	2
Claims	3	6

	Applicant Arguments/Remarks Made in an Amendment		7		7
	Abstract		8		8
Warnings:					
Information:					
6	Application Data Sheet	APP_-_ADS.pdf	1826367 26d827dfe93e63ed4a8ce69326d03001cfb6a8e1	no	9
Warnings:					
Information:					
7	Information Disclosure Statement (IDS) Form (SB08)	APP_-_IDS_1st_SB08.pdf	378429 06745817b4f5654f6e640bb52decfad5dd92aeb9	no	3
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
8	Documents submitted with 371 Applications	ISR_WrittenOpinion.pdf	1235126 8bbbbca747df64154d5e654893f5dfedb994c224	no	9
Warnings:					
Information:					
9	Foreign Reference	EP2924603A2.pdf	1295432 33e96054a1f884cfc135be2370966b0f950f4149	no	17
Warnings:					
Information:					
10	Foreign Reference	WO2016083216A1.pdf	1376939 d1a08e09d1d90e4d0615fa184c75b4ab186a9c44	no	20
Warnings:					
Information:					
11		Specification.pdf	1140836 b0a7d95554c98b7f260db25d30e372b450d23969	yes	25
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**		**End**

	Specification		1	20	
	Claims		21	24	
	Abstract		25	25	
Warnings:					
Information:					
12	Drawings-only black and white line drawings	Drawings.pdf	56002 5298b6d1276e40304d512aabaf089446889 74ce5	no	2
Warnings:					
Information:					
13	Documents submitted with 371 Applications	PCT_Docs.pdf	830621 24cebeea49297134d67a9dc6ca584228ac3 c5cfd	no	4
Warnings:					
Information:					
14	Documents submitted with 371 Applications	Article_19_Amended_Claims.pdf	904013 acb4bc4654bc3bc6c21e2bae8786ad89dd7 e04ea	no	7
Warnings:					
Information:					
15	Fee Worksheet (SB06)	fee-info.pdf	38403 71f003403575dc6c51adbfe94c4c8856255a 756f	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	12492782		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO-1390 (01-18)
Approved for use through 8/31/2019. OMB 0651-0021
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A SUBMISSION UNDER 35 U.S.C. 371

Attorney Docket No.	
1032326-001016	
U.S. Application No. (if known, see 37 CFR 1.5)	

International Application No.	International Filing Date	Priority Date Claimed
PCT/EP2018/081759	2018-11-19	2017-12-29

Title of Invention
AUTHENTICATION METHOD, DEVICE AND SYSTEM

First Named Inventor
Fabrice DELHOSTE

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information.

1. ☐ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). NOTE: The express request under 35 U.S.C. 371(f) will not be effective unless the requirements under 35 U.S.C. 371(c)(1), (2), and (4) for payment of the basic national fee, copy of the International Application and English translation thereof (if required), and the oath or declaration of the inventor(s) have been received.
2. ☑ A copy of the International Application (35 U.S.C. 371(c)(2)) is attached hereto (not required if the International Application was previously communicated by the International Bureau or was filed in the United States Receiving Office (RO/US)).
3. An English language translation of the International Application (35 U.S.C. 371(c)(2))
   a. ☐ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
4. An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4))
   a. ☐ is attached.
   b. ☐ was previously filed in the international phase under PCT Rule 4.17(iv).

Items 5 to 8 below concern amendments made in the international phase.

PCT Article 19 and 34 amendments

5. ☑ Amendments to the claims under PCT Article 19 are attached (not required if communicated by the International Bureau) (35 U.S.C. 371(c)(3)).
6. ☐ English translation of the PCT Article 19 amendment is attached (35 U.S.C. 371(c)(3)).
7. ☐ English translation of annexes (Article 19 and/or 34 amendments only) of the International Preliminary Examination Report is attached (35 U.S.C. 371(c)(5)).

Cancellation of amendments made in the international phase

8a. ☑ Do not enter the amendment made in the international phase under PCT Article 19.

8b. ☐ Do not enter the amendment made in the international phase under PCT Article 34.

NOTE: A proper amendment made in English under Article 19 or 34 will be entered in the U.S. national phase application absent a clear instruction from applicant not to enter the amendment(s).

The following items 9 to 17 concern a document(s) or information included.

9. ☑ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
10. ☑ A preliminary amendment.
11. ☑ An Application Data Sheet under 37 CFR 1.76.
12. ☐ A substitute specification. NOTE: A substitute specification cannot include claims. See 37 CFR 1.125(b).
13. ☑ A power of attorney and/or change of address letter.
14. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.3 and 37 CFR 1.821-1.825 (not required if sequence listing in text format was indicated on the PCT Request as part of the International Application and the sequence listing was published as part of the international application).
15. ☐ Assignment papers *(cover sheet and document(s))*. Name of Assignee: THALES DIS FRANCE SA
16. ☐ 37 CFR 3.73(c) Statement *(when there is an Assignee)*.

This collection of information is required by 37 CFR 1.414 and 1.491-1.492. The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 15 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

U.S. APPLN. No. (if known – see 37 CFR 1.5)	INTERNATIONAL APPLICATION No.	ATTORNEY DOCKET No.
	PCT/EP2018/081759	1032326-001016

17. ☐ Other items or information:

The following fees have been submitted.	CALCULATIONS
18. ☑ Basic national fee (37 CFR 1.492(a)) **$300**	$300.00
19. ☑ Examination fee (37 CFR 1.492(c)) • If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4)..... **$0** • All other situations **$760**	760.00 $
20. ☑ Search fee (37 CFR 1.492(b)) • If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4)..... **$0** • Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority ..... **$140** • International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB..... **$520** • All other situations **$660**	520.00 $
TOTAL OF 18, 19, and 20 =	$1580.00
☐ Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing in compliance with 37 CFR 1.821(c) or (e) in an electronic medium or computer program listing in an electronic medium) (37 CFR 1.492(j)). Fee for each additional 50 sheets of paper or fraction thereof **$400**	

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof (round **up** to a whole number)	RATE	
27 - 100 =	/ 50 =		x **$400**	$

Surcharge for furnishing any of the search fee, examination fee, or the oath or declaration after the date of commencement of the national stage (37 CFR 1.492(h)).....**$140**	$140.00

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total claims	10 - 20 =	0	x **$100**	$0.00
Independent claims	4 - 3 =	1	x **$460**	$460.00
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			**+ $820**	$

Fee for submission of Sequence Listing text file of 300 MB to 800 MB (37 CFR 1.21(o)(1))..... **$1,000**	$
Fee for submission of Sequence Listing text file of more than 800 MB (37 CFR 1.21(o)(2))..... **$10,000**	$
Processing fee for furnishing the English translation later than 30 months from the earliest claimed priority date (37 CFR 1.492(i))..... **$140 +**	$
TOTAL OF ABOVE CALCULATIONS =	$ 2180.00
☐ **Applicant asserts small entity status.** See 37 CFR 1.27. Fees above are reduced by ½.	
☐ **Applicant certifies micro entity status.** See 37 CFR 1.29. Fees above are reduced by ¾. Applicant must attach form PTO/SB/15A or B or equivalent.	
TOTAL NATIONAL FEE =	$2180.00
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31)..... **$50.00** per property **+**	$
TOTAL FEES ENCLOSED =	$2180.00

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees.

c. ☑ The Director is hereby authorized to charge additional fees which may be required, or credit any overpayment, to Deposit Account No. 02-4800 as follows:

i. ☐ any required fee.

ii. ☑ any required fee except for excess claims fees required under 37 CFR 1.492(d) and (e) and multiple dependent claim fee required under 37 CFR 1.492(f).

d. ☑ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038. The PTO-2038 should only be mailed or faxed to the USPTO. However, when paying the basic national fee, the PTO-2038 may NOT be faxed to the USPTO.

ADVISORY: If filing by EFS-Web, do **NOT** attach the PTO-2038 form as a PDF along with your EFS-Web submission. Please be advised that this is **not** recommended and by doing so your **credit card information may be displayed via PAIR**. To protect your information, it is recommended to pay fees online by using the electronic payment method.

NOTE: Where an appropriate time limit under 37 CFR 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the International Application to pending status.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013, and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

NOTE 1: By providing this statement under 37 CFR 1.55 or 1.78, **this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA**.

NOTE 2: A U.S. national stage application may not claim priority to the international application of which it is the national phase. The filing date of a U.S. national stage application is the international filing date. See 35 U.S.C. 363.

Correspondence Address

☑ The address associated with Customer Number: 21839 **OR** ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone			
Email					

Signature	/James A LaBarre/	Date	June 26, 2020
Name (Print/Type)	James A. LaBarre	Registration No. (Attorney/Agent)	28,632

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc Code: ECOMM.AUTH/ECOMM.WTDW
Doc Description: Internet Communications Authorized/Internet Communications Authorization Withdrawn

PTO/SB/439 (11-15)

AUTHORIZATION FOR INTERNET COMMUNICATIONS IN A PATENT APPLICATION OR REQUEST TO WITHDRAW AUTHORIZATION FOR INTERNET COMMUNICATIONS		
	Application No.	
	Filing Date	
	First Named Inventor	Fabrice DELHOSTE
	Art Unit	
	Examiner Name	
	Practitioner Docket No.	1032326-001016

To: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I. To authorize permission for Internet Communications.

☑ Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with the undersigned and practitioners in accordance with 37 CFR 1.33 and 37 CFR 1.34 concerning any subject matter of this application via video conferencing, instant messaging, or electronic mail. I understand that a copy of these communications will be made of record in the application file. (MPEP 502.03)

II. To withdraw authorization for Internet Communications.

☐ The authorization given on _____, to the USPTO to communicate with the undersigned and any practitioner in accordance with 37 CFR 1.33 and 37 CFR 1.34 concerning any subject matter of this application via Internet communications such as video conferencing, instant messaging, or electronic mail is hereby withdrawn. I understand that the withdrawal is effective when approved rather than when received.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 28,632.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/James A LaBarre/ — Signature

June 26, 2020 — Date

James A. LaBarre — Typed or printed name

703-838-6648 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Juristic entities must be represented by a patent practitioner (see 37 CFR 1.31, which is applicable to any paper filed on or after September 16, 2012, that is presented on behalf of a juristic entity, regardless of application filing date). Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Patent
Attorney Docket No. 1032326-001016

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Fabrice DELHOSTE	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Confirmation No.: Unassigned
	)	
Filing Date: On Even Date Herewith	)	
	)	
Title: AUTHENTICATION METHOD, DEVICE AND SYSTEM	)	
	)	
	)	

GENERAL AUTHORIZATION FOR PETITIONS FOR EXTENSIONS OF TIME AND PAYMENT OF FEES

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

In accordance with 37 C.F.R. § 1.136(a)(3), the U.S. Patent and Trademark Office is hereby provided with a general authorization to treat any concurrent or future reply requiring a petition for an extension of time for its timely submission as containing a request therefor for the appropriate length of time.

The Commissioner is hereby authorized to charge any appropriate fees that may be required by this paper, or any other submissions in this application, and to credit any overpayment, to Deposit Account No. 02-4800.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: June 26, 2020 By: /James A LaBarre/
James A. LaBarre
Registration No. 28,632

Customer No. 21839
T 703 836 6620

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 01/31/2018. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	
Filing Date	
First Named Inventor	Fabrice DELHOSTE
Title	AUTHENTICATION METHOD, DEVICE AND SYSTEM
Art Unit	
Examiner Name	
Attorney Docket Number	1032326-001016

SIGNATURE of Applicant or Patent Practitioner

Signature	/James A LaBarre/	Date (Optional)	June 26, 2020
Name	James A. LaBarre	Registration Number	28,632
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)	THALES DIS FRANCE SA		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 21839

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

THALES DIS FRANCE SA

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	
Name	MOUCHART Patrick		
Title	Chief Executive Officer		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Fabrice DELHOSTE	Group Art Unit: Unassigned
Application No.: Unassigned	Examiner: Unassigned
Filed: On Even Date Herewith	Confirmation No.: Unassigned
For: AUTHENTICATION METHOD, DEVICE AND SYSTEM	

PRELIMINARY AMENDMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

Prior to examination of the above-captioned patent application, kindly amend the application as follows:

AMENDMENTS TO THE ABSTRACT:

Please replace the original Abstract with the following amended Abstract of the Disclosure. This new Abstract of the Disclosure is also set forth on a separate sheet attached to the end of this Preliminary Amendment:

ABSTRACT OF THE DISCLOSURE

The invention relates to an authentication method. The method comprises: [[-]] collecting ~~24~~, based on a predetermined authentication policy, at least one context data element; [[-]] constituting ~~28~~, based on the at least one collected context data element, a data packet; [[-]] generating ~~216~~, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash; [[-]] sending the generated hash; [[-]] generating ~~220~~, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and [[-]] authenticating ~~224~~ successfully or not ~~223~~ based on the generated hash distance, as an authentication step. The invention also relates to corresponding device and system.

~~Figure 2~~

AMENDMENTS TO THE CLAIMS:

The following listing of claims will replace all prior versions and listings of claims in this application.

LISTING OF CLAIMS:

Claims 1-15 Cancelled.

16. (New) An authentication method comprising:

- collecting, based on a predetermined authentication policy, at least one context data element;
- constituting a data packet, based on the at least one collected context data element;
- generating a hash, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm;
- sending the generated hash;
- generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and
- authenticating successfully or not based on the generated hash distance, as an authentication step.

17. (New) The method according to claim 16, wherein, the predetermined hash type algorithm comprises a locality sensitive hash type algorithm, and wherein the method further comprises, as the hash distance generation step and the authentication step, the following steps:

- generating a score, by using the locality sensitive hash type algorithm, as a level of similarity between the generated hash and the predetermined reference hash;
- comparing the score to a predetermined threshold value;

- authenticating successfully only if the score is equal to or greater than the predetermined threshold value.

18. (New) The method according to claim 16, wherein, prior to generating the hash, the method further comprises sorting, according to a numerical order, the at least one collected context data element within the data packet.

19. (New) The method according to claim 16, wherein, prior to generating the hash, the method further comprises weighting, according to the authentication policy, the at least one context data element.

20. (New) The method according to claim 16, wherein, prior to constituting the data packet, the method further comprises grouping together, according to the authentication policy, at least two context data elements comprised within the at least one context data element, to constitute at least one corresponding context data group.

21. (New) The method according to claim 16, wherein, prior to generating the hash, the method further comprises ciphering the data packet, according to the authentication policy.

22. (New) The method according to claim 21, wherein a key used for the data packet ciphering includes a key generated by using a hash-based message authentication code key type derivation function.

23. (New) A first authentication device, wherein the first authentication device is configured to:

- collect at least one context data element, based on a predetermined authentication policy;
- constitute a data packet, based on the at least one collected context data element;
- generate a hash, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm; and
- send the generated hash to a second authentication device.

24. (New) A second authentication device, wherein the second authentication device is configured to:

- receive a generated hash;
- generate a hash distance between the generated hash and a predetermined reference hash; and
- authenticate successfully or not based on the generated hash distance.

25. (New) An authentication system, comprising a first authentication device and at least one second authentication device, wherein the first authentication device is configured to:

- collect at least one context data element, based on a predetermined authentication policy;
- constitute a data packet, based on the at least one collected context data element;
- generate a hash, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm; and
- send to the second authentication device, the generated hash;
    - and wherein the second authentication device is configured to:
- receive the generated hash from the first device;

- generate a hash distance between the generated hash and a predetermined reference hash; and

- authenticate successfully or not based on the generated hash distance.

REMARKS

The claims presented herein substantively correspond to the claims presented in the Article 19 Amendment submitted in the corresponding international application, having been revised to remove informalities and multiple dependencies. No new matter is introduced by these changes.

Favorable consideration of the application in view of the foregoing amendments is respectfully requested. Should any questions arise in connection with this application, it is respectfully requested that the undersigned be contacted at the number indicated below.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date June 26, 2020

By: /James A LaBarre/
James A. LaBarre
Registration No. 28,632

Customer No. 21839
703 836 6620

ABSTRACT OF THE DISCLOSURE

The invention relates to an authentication method. The method comprises: collecting, based on a predetermined authentication policy, at least one context data element; constituting, based on the at least one collected context data element, a data packet; generating, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm, a hash; sending the generated hash; generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash; and authenticating successfully or not based on the generated hash distance, as an authentication step. The invention also relates to corresponding device and system.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	1032326-001016
	Application Number	
Title of Invention	AUTHENTICATION METHOD, DEVICE AND SYSTEM	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Fabrice		DELHOSTE	

Residence Information (Select One) US Residency ● Non US Residency Active US Military Service

City	Gemenos	Country of Residence [i]	FR

Mailing Address of Inventor:

Address 1	c/o GEMALTO SA, Service Brevets		
Address 2	525 avenue du Pic de Bertagne CS12023		
City	Gemenos	State/Province	
Postal Code	13881	Country [i]	FR

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Frédéric		PAILLART	

Residence Information (Select One) US Residency ◉ Non US Residency Active US Military Service

City	Gemenos	Country of Residence [i]	FR

Mailing Address of Inventor:

Address 1	c/o GEMALTO SA, Service Brevets		
Address 2	525 avenue du Pic de Bertagne CS12023		
City	Gemenos	State/Province	
Postal Code	13881	Country [i]	FR

Inventor 3 Remove

Legal Name

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	1032326-001016
	Application Number	
Title of Invention	AUTHENTICATION METHOD, DEVICE AND SYSTEM	

Prefix	Given Name	Middle Name	Family Name	Suffix
	Sébastien		PETIT	

Residence Information (Select One) US Residency ◉ Non US Residency Active US Military Service

City	Gemenos	Country of Residence [i]	FR

Mailing Address of Inventor:

Address 1	c/o GEMALTO SA, Service Brevets
Address 2	525 avenue du Pic de Bertagne CS12023

City	Gemenos	State/Province	
Postal Code	13881	**Country** [i]	FR

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	21839		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	AUTHENTICATION METHOD, DEVICE AND SYSTEM		
Attorney Docket Number	1032326-001016	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	2	**Suggested Figure for Publication (if any)**	2

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country [i]

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	1032326-001016
	Application Number	
Title of Invention	AUTHENTICATION METHOD, DEVICE AND SYSTEM	

Publication Information:

☐	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐	**Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	● Customer Number	US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	21839		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	a 371 of international	PCT/EP2018/081759	2018-11-19

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	1032326-001016
	Application Number	
Title of Invention	AUTHENTICATION METHOD, DEVICE AND SYSTEM	

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)
17306977.4	EP	2017-12-29	

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	1032326-001016
	Application Number	
Title of Invention	AUTHENTICATION METHOD, DEVICE AND SYSTEM	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	1032326-001016
	Application Number	
Title of Invention	AUTHENTICATION METHOD, DEVICE AND SYSTEM	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 — Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

● Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.	Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☑

Organization Name	THALES DIS FRANCE SA		
Mailing Address Information For Applicant:			
Address 1	6, rue de la Verrerie		
Address 2			
City	Meudon	**State/Province**	
Country	FR	Postal Code	92190
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	1032326-001016
	Application Number	
Title of Invention	AUTHENTICATION METHOD, DEVICE AND SYSTEM	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☑

Organization Name	THALES DIS FRANCE SA

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1	6, rue de la Verrerie		
Address 2			
City	Meudon	**State/Province**	
Country i	FR	Postal Code	92190
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/James A LaBarre/			Date (YYYY-MM-DD)	2020-06-26
First Name	James	Last Name	LaBarre	Registration Number	28632

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	1032326-001016
	Application Number	
Title of Invention	AUTHENTICATION METHOD, DEVICE AND SYSTEM	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1 The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3 A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent CooperationTreaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.