US 20020046336A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2002/0046336 A1

Kon et al. (43) Pub. Date: Apr. 18, 2002

(54) INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING METHOD, AND PROGRAM PROVIDING MEDIUM

(75) Inventors: **Masashi Kon**, Kanagawa (JP); **Yoshihito Ishibashi**, Tokyo (JP); **Shinako Matsuyama**, Tokyo (JP); **Ichiro Futamura**, Kanagawa (JP); **Hideaki Watanabe**, Tokyo (JP)

Correspondence Address:
Sonnenschein, Nath & Rosenthal
P.O. Box #061080
Wacker Drive Station - Sear Tower
Chicago, IL 60606 (US)

(73) Assignee: **Sony Corporation**

(21) Appl. No.: **09/944,961**

(22) Filed: **Aug. 30, 2001**

(30) **Foreign Application Priority Data**

Aug. 31, 2000 (JP) P2000-264517

Publication Classification

(51) **Int. Cl.**[7] **H04L 9/32**

(52) **U.S. Cl.** **713/156**; 713/182; 713/169

(57) **ABSTRACT**

Disclosed are an information processing apparatus and an information processing method which execute person authentication and allows various services such as receiving of contents to be received, provided that the authentication is successfully passed. In the information processing apparatus for executing, by a connection to an external server providing various services such as contents transmission, a process such as receiving of contents, person authentication is executed by comparing a template acquired from a person identification certificate storing a template which is person identification data of a user using the information processing apparatus with sampling information input by the user, and a connection to the external server is executed provided that the authentication is successfully passed. In addition, the person identification certificate and the public key certificate are stored in a memory together with link information in which the person identification certificate and the public key certificate applied during a process of establishing a connection to the server are related to each other.

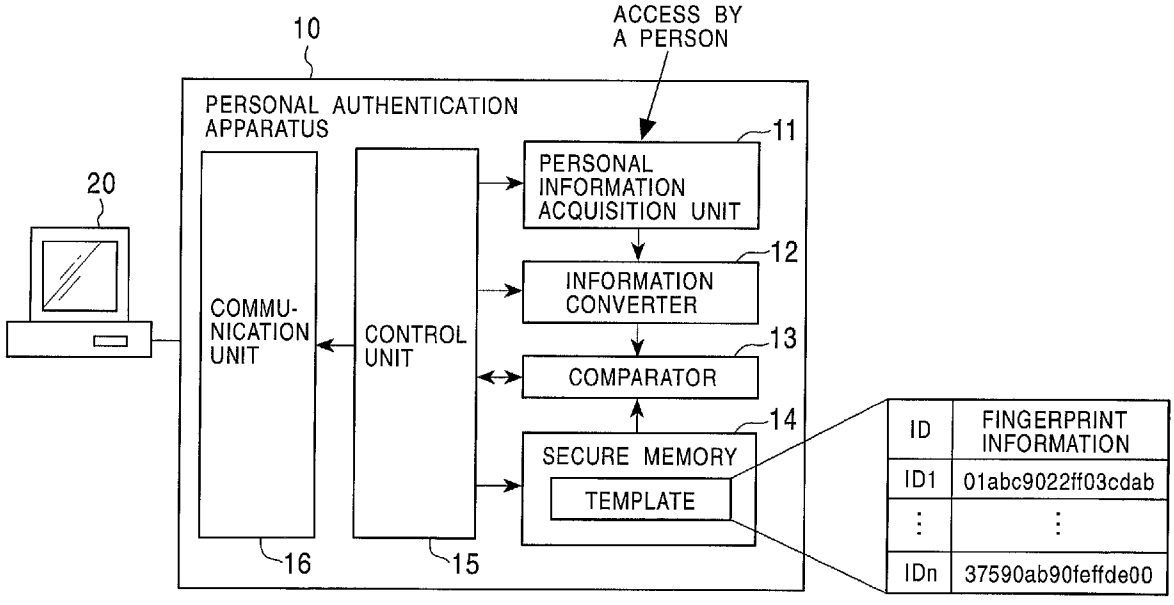


FIG. 1

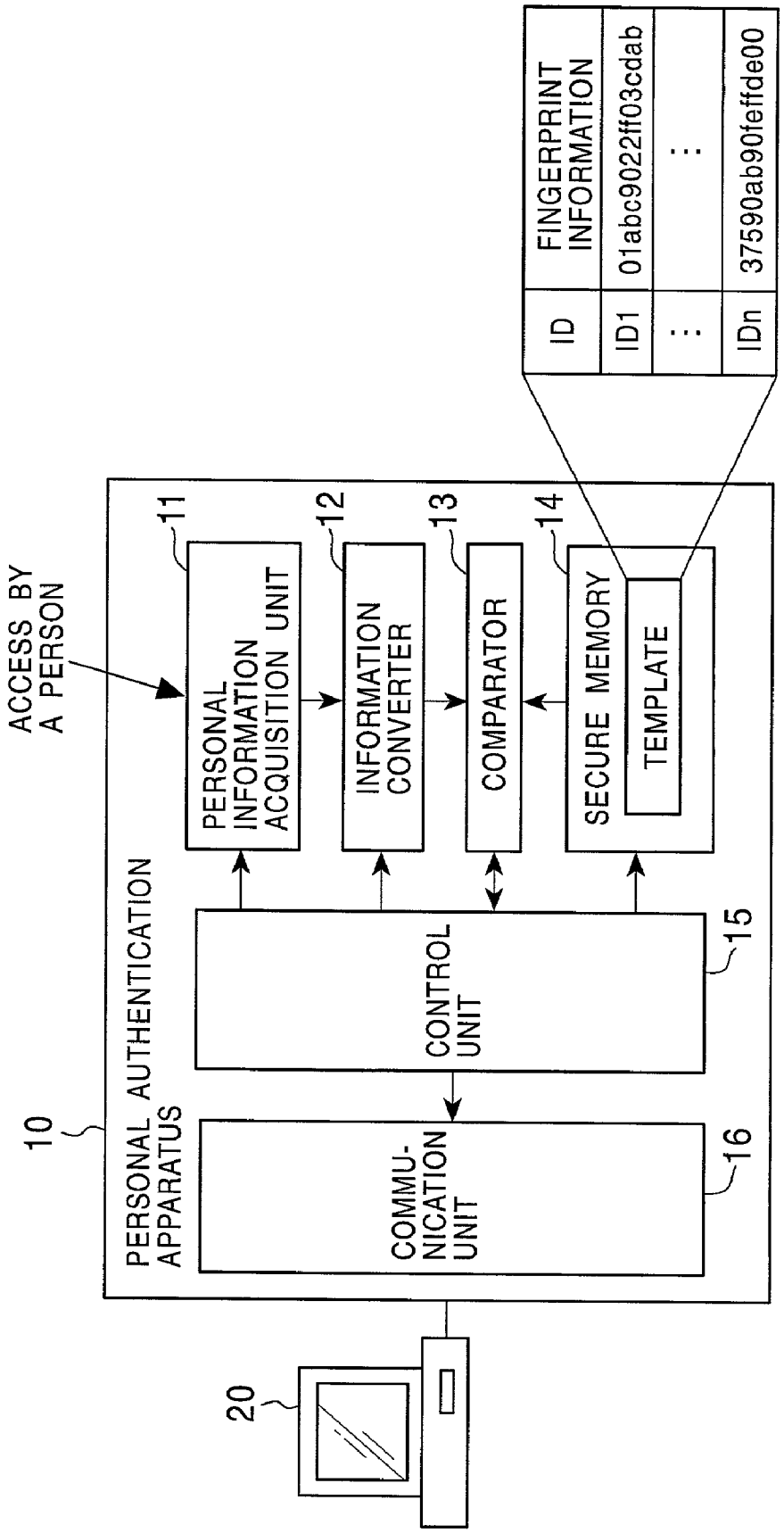

ACCESS BY A PERSON
PERSONAL AUTHENTICATION APPARATUS
10
PERSONAL INFORMATION ACQUISITION UNIT
11
INFORMATION CONVERTER
12
COMPARATOR
13
SECURE MEMORY
14
TEMPLATE
CONTROL UNIT
15
COMMU-NICATION UNIT
16
20
ID
FINGERPRINT INFORMATION
ID1
01abc9022ff03cdab
IDn
37590ab90feffde00

FIG. 2

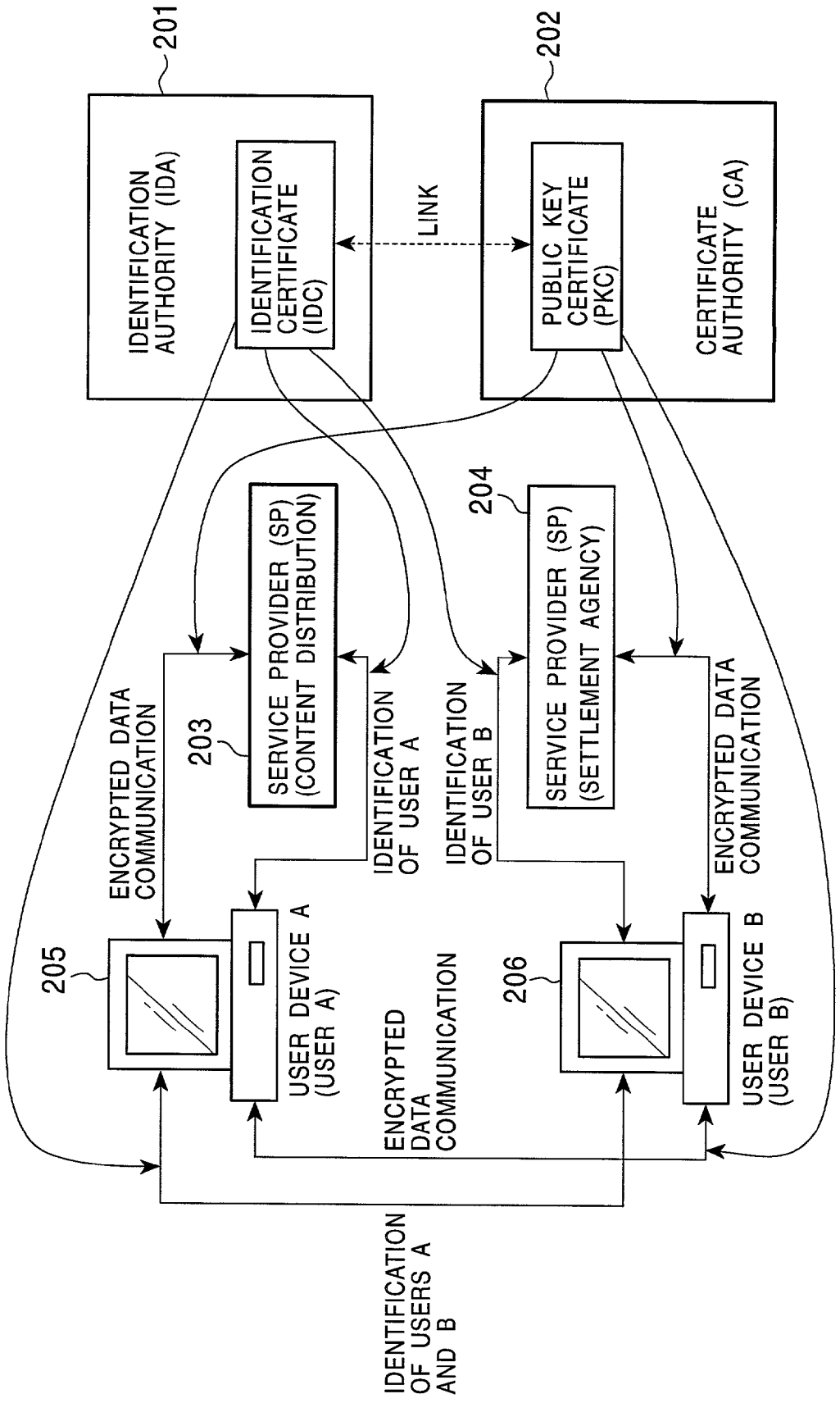

201
IDENTIFICATION AUTHORITY (IDA)
IDENTIFICATION CERTIFICATE (IDC)
LINK
202
PUBLIC KEY CERTIFICATE (PKC)
CERTIFICATE AUTHORITY (CA)
203
SERVICE PROVIDER (SP) (CONTENT DISTRIBUTION)
204
SERVICE PROVIDER (SP) (SETTLEMENT AGENCY)
ENCRYPTED DATA COMMUNICATION
IDENTIFICATION OF USER A
IDENTIFICATION OF USER B
ENCRYPTED DATA COMMUNICATION
205
USER DEVICE A (USER A)
ENCRYPTED DATA COMMUNICATION
206
USER DEVICE B (USER B)
IDENTIFICATION OF USERS A AND B

FIG. 3

Item	Description	Value employed in the present IA
Version 1		
version	Version of the certificate format	V3
serial Number	Serial number of the certificate assigned by the IA	Assigned in a serial fashion
signature algorithm Identifier algorithm parameters	Algorithm of the signature of the certificate and parameters thereof	Elliptic curve number/RSA parameters when an elliptic curve is used Key length when RSA is employed
issuer	IA name (in a distiguished name form)	Name of the present IA
validity notBefore notAfter	Period during which the certificate is valid Start date Expiration date	
subject	Name which identifies the user	User device ID or ID of the service subject
subject Public Key Info algorithm subject Public key	Information of the public key of the user Algorithem of the key Key	 Elliptic curve/RSA Public key of the user
Version 3		
authority Key Identifier key Identifier authority Cert Issuer authority Cert Serial Number	Key identifier used in verification of the IA Key identification number (octal number) Name of the IA (in a general name form) Identification number	
subject key Identifier	Used when a plurality of keys are certified	Not used
key usage (0)digital Signature (1)non Repudiation (2)key Encipherment (3)data Encipherment (4)key Agreement (5)key CertSign (6)cRL Sign	Specifying the purpose of the key (0)for digital signature (1)to prevent repudiation (2)for encryption of the Key (3)for encryption of a message (4)for use in transmission of a symmetric key (5)used to verify the certificate (6)used to verify the signature of the certificate revolution list	0,1,4, or 6 is used
private Key Usage Period notBefore notAfter	Period during which the private key stored in the user is valid	Usage period is the same for the certificate, the public key, and the private Key (default)

FIG. 4

Certificate Policy policy Identifier policy Qualifers	Certificate policy of the certificate authority Policy ID (according to ISO/IEC9834-1) Certification criteria	
policy Mappings issuer Domain Policy subject Domain Policy	Required only when the CA is certificated. Mappings of the policy of the issuer domain policy and the subject domain policy are defined	default = none
supported Algorithms algorithm Identifier intended Usage intended Certificate Policies	Attributes of the directory (X.500) are defined. Used to inform a receiving party of communication of the attributes the direction so that the receiving party can use the direction information	default = none
subject Alt Name	Alternative name of the user (in the form of GN)	not used
issuer Alt Name	Not used although this item is included in the certificate format (default = none)	default = none
subject Directory Attributes	Arbitrary attributes of the user	not used
basic Constraints	Specifies the public key to be certified	
cA path Len Constraint	Indicates whether the public key is used by a user or by a certificate authority to write a signature	default = used by a user
name Constraints permitted Subtrees base minimum	Used only when the certification is to certify a certification authority (CA)	default = none
maximum excluded Subtrees		
policy Constraints requier Explicit Policy inhibit Policy Mapping	Constraints are described in terms of requirements of explicit policy ID or inhibit policy mapping for the remaining certification path	
CRL Distribution Points	Indicates a reference point in the revocation list at which data is present which indicates whether the certificate of a user is revocated	Pointer which points to a location where the certificate is registered. The revocation list is managed by an issuer
Signature	Signature of the issuer	

FIG. 5

	Item	Description
Indis-pensable Items	Version	Version
	Serial Number	Identification Number
	signature algorithm Identifier algorithm parameters	Signature algorithem Algorithm Parameters
	Issuer	Name of the identification authority (in the form of a distinguished name)
	Validity notBefore notAfter	Period during which the certificate is valid Start date Expiration date
	Subject	Name of the subject to be certificated (in a DN form)
Extended Items	subject Template Info encrypt Type encrypt Unique ID encryption Algorithm parameter validity subject Template Source subject Template	Template information • encrypt Type • The unique ID or the certificate number of a public key certificate used for encryption • Algorithm • parameter • Validity period (start date, expiration date) • Type of the template • Template
	Subject PKC info subject PKC serial Number subject PKC Unique ID	Information about the public key certificate of the subject • Certificate number of the subject public key certificate • Unique ID of the subject of the subject public key certificate
	Issuer Unique ID	Unique ID of the issuer
	Subject Unique ID	Unique ID of the subject
	Public Key Certificate	Public key certificate
	Issuer Alt Name	Alternative name of the issuer
	subject Directory Attributes	Personal information (encrypted as required) information used to authenticate subject Age, sex, etc.
	Valid Count	Number of times the certificate is allowed to be used
	Control Table Link Info Ctl Tbl Location Ctl Tbl Unique ID	Link information describing group information • Location of a link information control table (URL, IP address, etc.) • Identification number of the link information
Indispen-sable	IDA Signature	Signature of the IDA

FIG. 6A

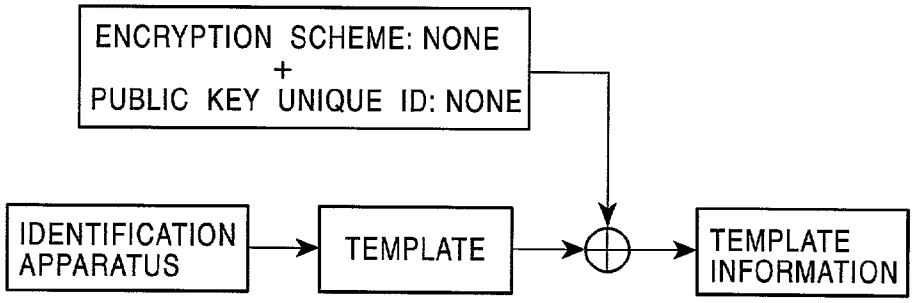


FIG. 6B

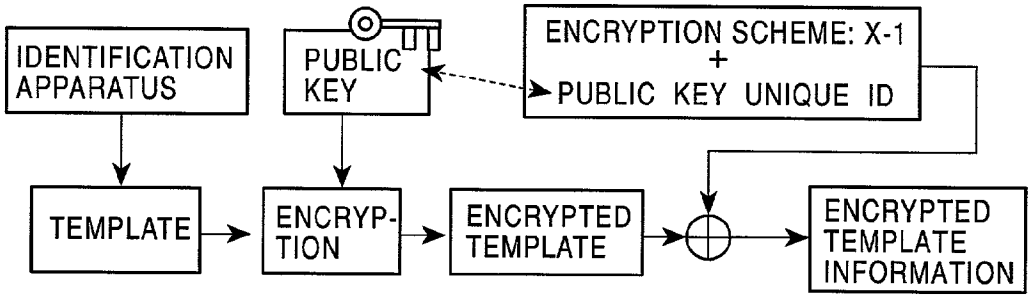


FIG. 6C

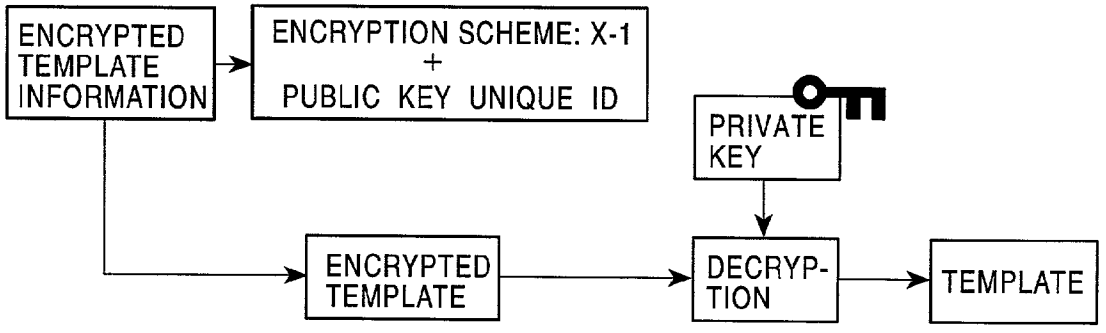


FIG. 7

PUBLIC KEY USED TO ENCRYPT TEMPLATES	EXAMPLES OF MANNERS IN WHICH TEMPLATE INFORMATION STORAGE IDC IS USED
PUBLEC KEY OF A USER OR A USER DEVICE	TO IDENTIFY AN AUTHORIZED USER OF A USER DEVICE (SUCH AS A PC) ON THE BASIS OF AN IDENTIFICATION CERTIFICATE OF THE USER
PUBLIC KEY OF A SERVICE PROVIDER	USED BY A SERVICE PROVIDER TO IDENTIFY A PARTICULAR USER SUCH AS A USER TO WHOM SERVICE IS TO BE PROVIDED, ON THE BASIS OF AN IDENTIFICATION CERTIFICATE (IDC) OF THE USER
PUBLIC KEY OF AN IDENTIFICATION AUTHORITY	IN DATA TRANSMISSION AMONG VARIOUS TERMINALS, A SENDER OR A RECEIVER IDENTIFIES

FIG. 8A

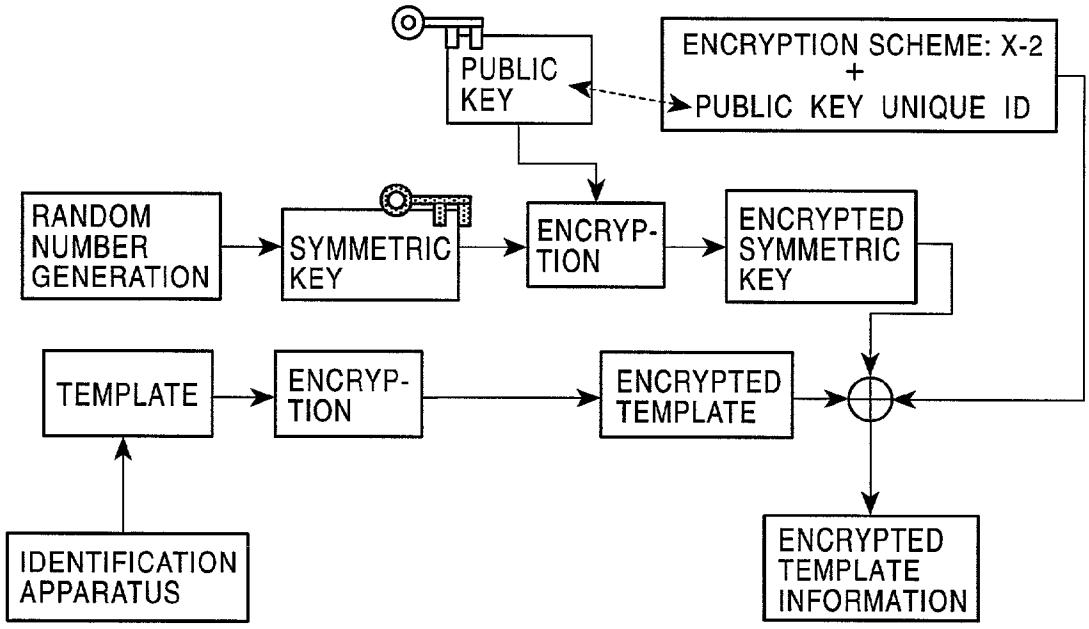

PUBLIC KEY
ENCRYPTION SCHEME: X-2 + PUBLIC KEY UNIQUE ID
RANDOM NUMBER GENERATION
SYMMETRIC KEY
ENCRYP-TION
ENCRYPTED SYMMETRIC KEY
TEMPLATE
ENCRYP-TION
ENCRYPTED TEMPLATE
IDENTIFICATION APPARATUS
ENCRYPTED TEMPLATE INFORMATION

FIG. 8B

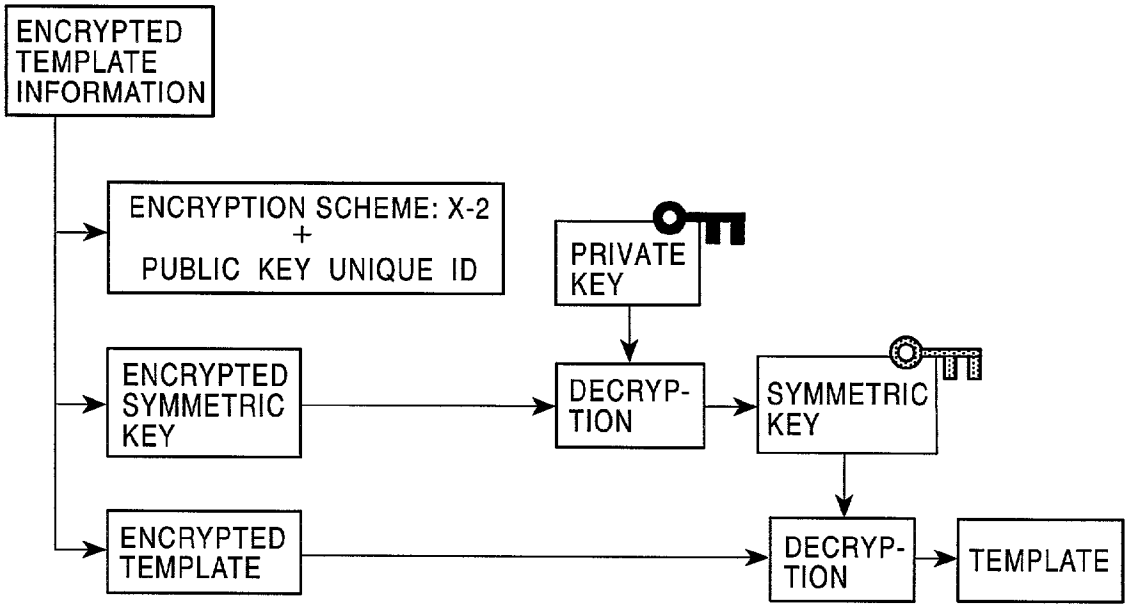

ENCRYPTED TEMPLATE INFORMATION
ENCRYPTION SCHEME: X-2 + PUBLIC KEY UNIQUE ID
PRIVATE KEY
ENCRYPTED SYMMETRIC KEY
DECRYP-TION
SYMMETRIC KEY
ENCRYPTED TEMPLATE
DECRYP-TION
TEMPLATE

FIG. 9

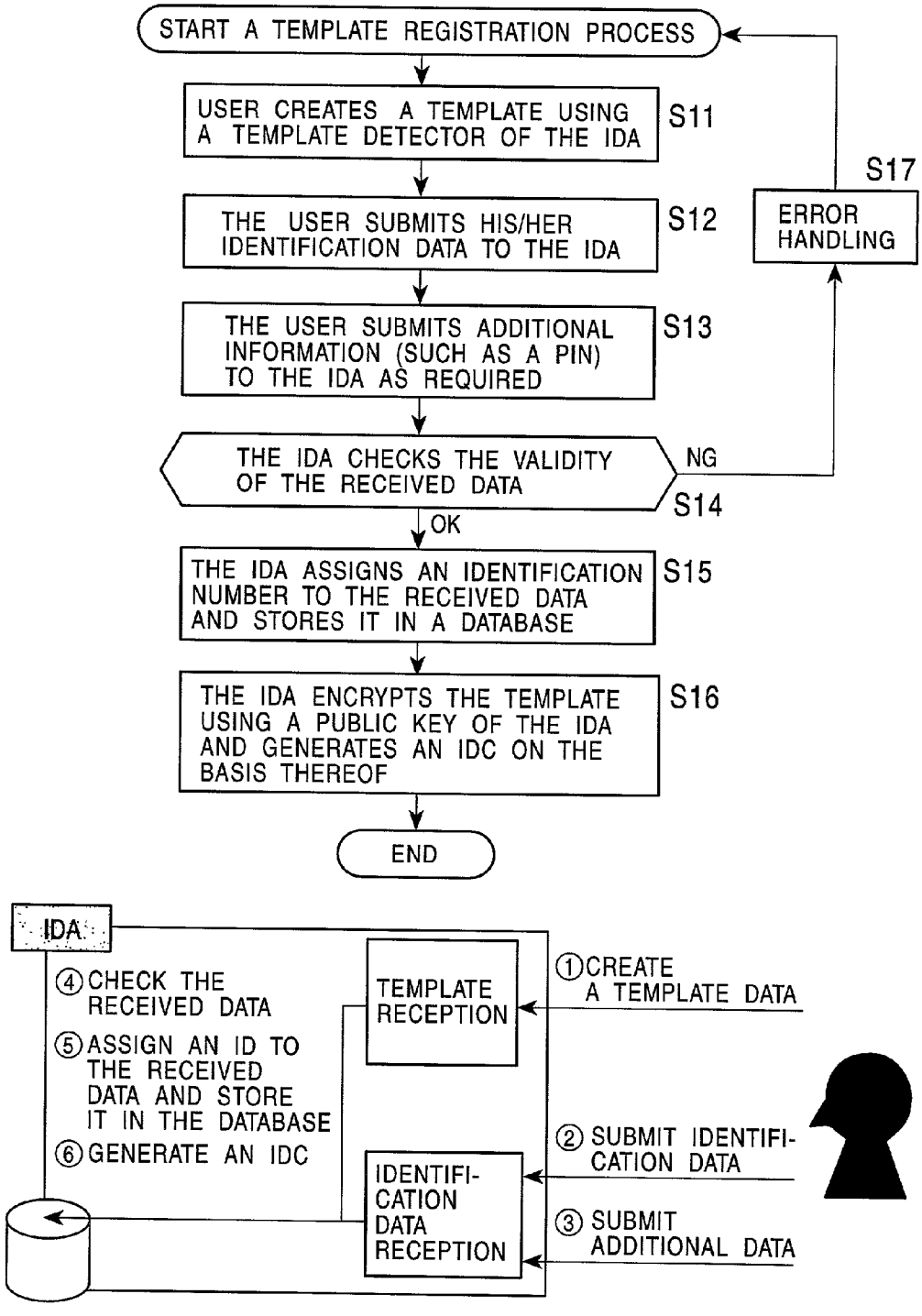
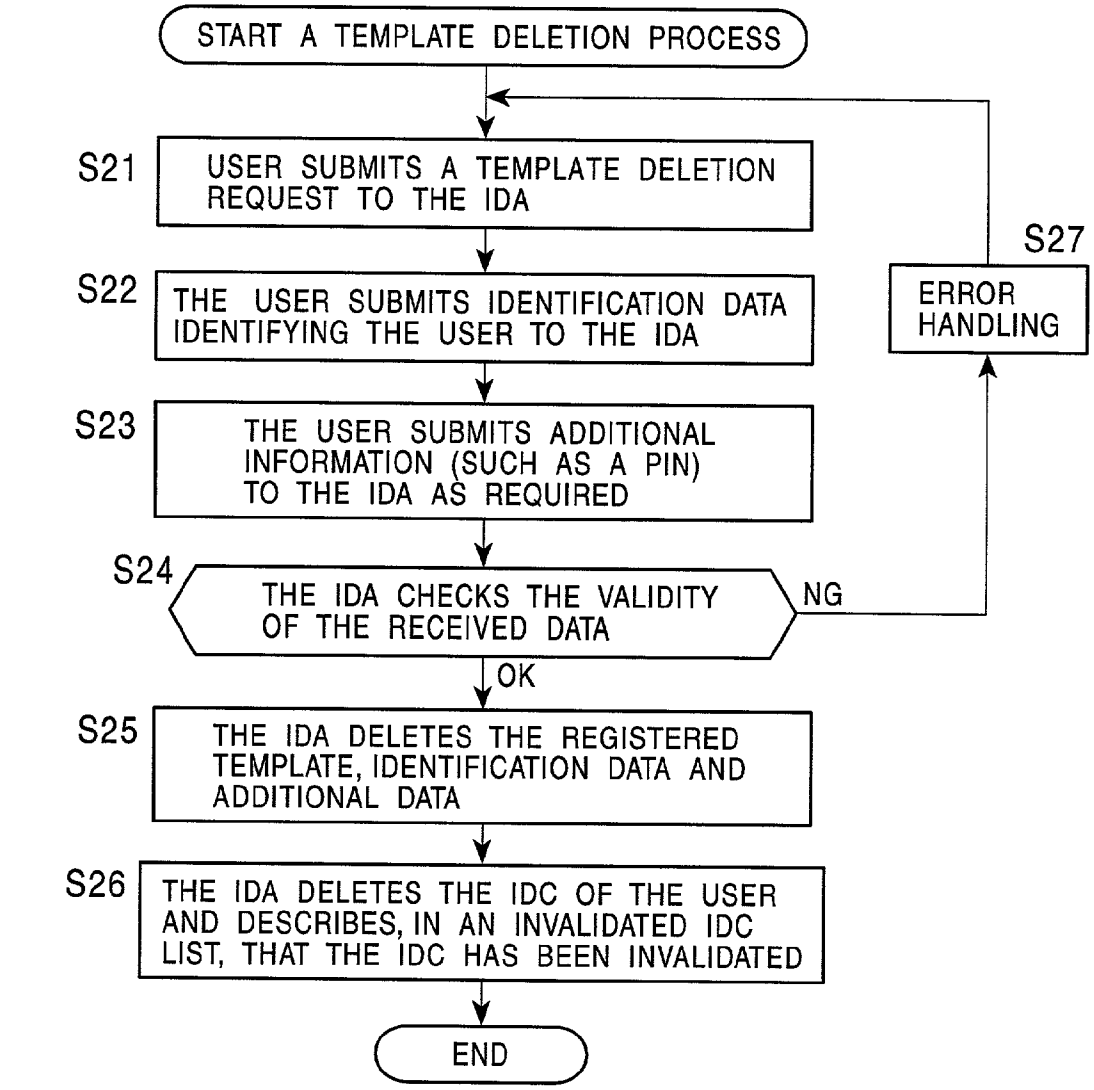

START A TEMPLATE REGISTRATION PROCESS
USER CREATES A TEMPLATE USING A TEMPLATE DETECTOR OF THE IDA
S11
THE USER SUBMITS HIS/HER IDENTIFICATION DATA TO THE IDA
S12
THE USER SUBMITS ADDITIONAL INFORMATION (SUCH AS A PIN) TO THE IDA AS REQUIRED
S13
THE IDA CHECKS THE VALIDITY OF THE RECEIVED DATA
NG
S14
OK
THE IDA ASSIGNS AN IDENTIFICATION NUMBER TO THE RECEIVED DATA AND STORES IT IN A DATABASE
S15
THE IDA ENCRYPTS THE TEMPLATE USING A PUBLIC KEY OF THE IDA AND GENERATES AN IDC ON THE BASIS THEREOF
S16
END
S17
ERROR HANDLING
IDA
④CHECK THE RECEIVED DATA
⑤ASSIGN AN ID TO THE RECEIVED DATA AND STORE IT IN THE DATABASE
⑥GENERATE AN IDC
TEMPLATE RECEPTION
IDENTIFI-CATION DATA RECEPTION
①CREATE A TEMPLATE DATA
② SUBMIT IDENTIFI-CATION DATA
③ SUBMIT ADDITIONAL DATA

FIG. 10


START A TEMPLATE DELETION PROCESS
S21
USER SUBMITS A TEMPLATE DELETION REQUEST TO THE IDA
S22
THE USER SUBMITS IDENTIFICATION DATA IDENTIFYING THE USER TO THE IDA
S23
THE USER SUBMITS ADDITIONAL INFORMATION (SUCH AS A PIN) TO THE IDA AS REQUIRED
S24
THE IDA CHECKS THE VALIDITY OF THE RECEIVED DATA
NG
S27
ERROR HANDLING
OK
S25
THE IDA DELETES THE REGISTERED TEMPLATE, IDENTIFICATION DATA AND ADDITIONAL DATA
S26
THE IDA DELETES THE IDC OF THE USER AND DESCRIBES, IN AN INVALIDATED IDC LIST, THAT THE IDC HAS BEEN INVALIDATED
END

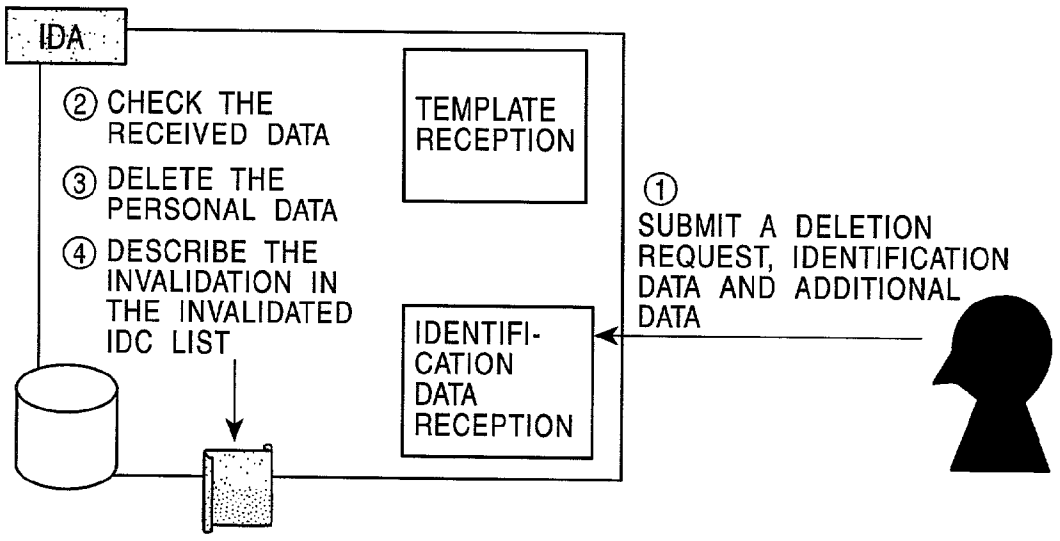

IDA
② CHECK THE RECEIVED DATA
③ DELETE THE PERSONAL DATA
④ DESCRIBE THE INVALIDATION IN THE INVALIDATED IDC LIST
TEMPLATE RECEPTION
IDENTIFI-CATION DATA RECEPTION
① SUBMIT A DELETION REQUEST, IDENTIFICATION DATA AND ADDITIONAL DATA

FIG. 11

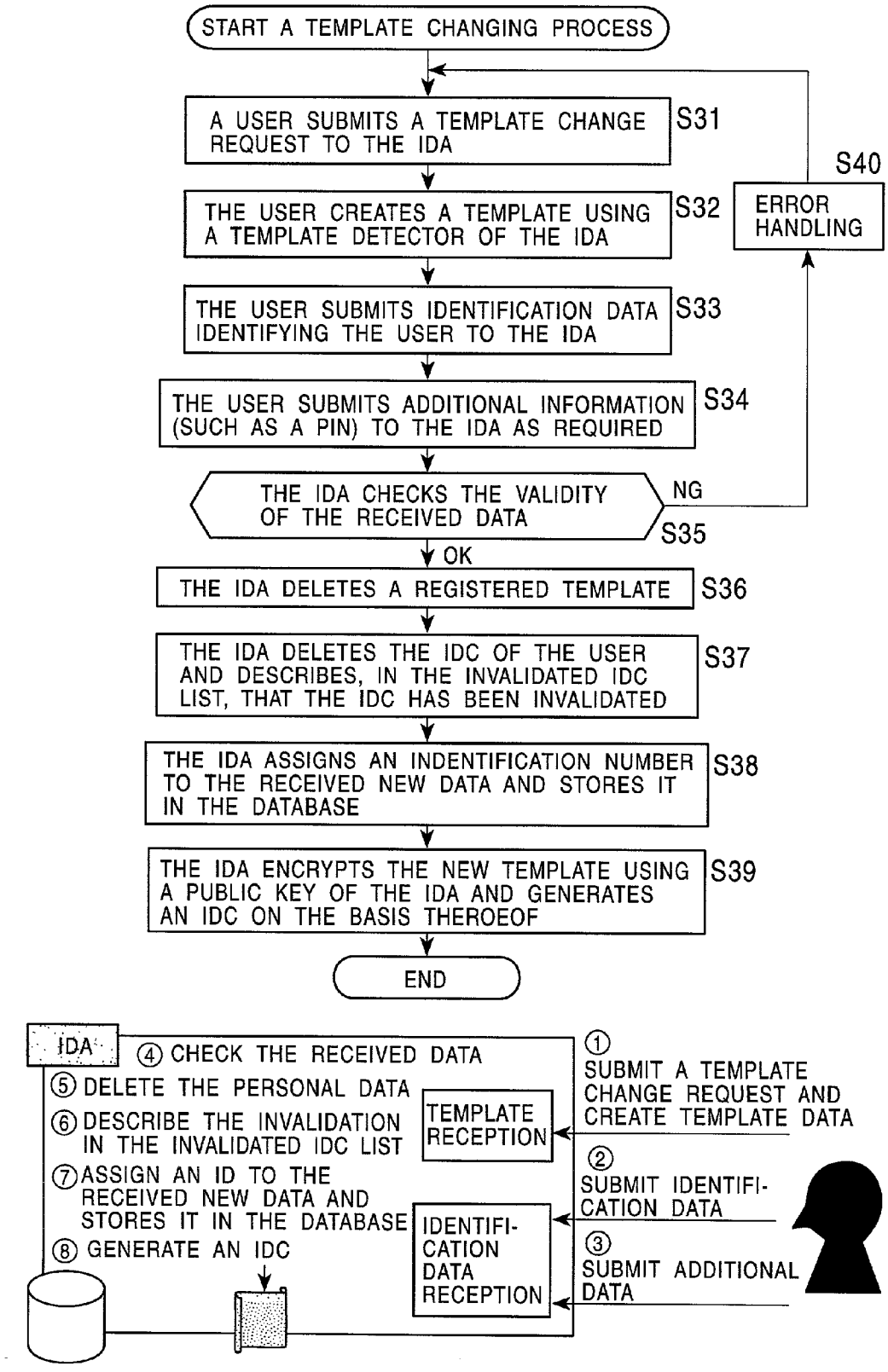
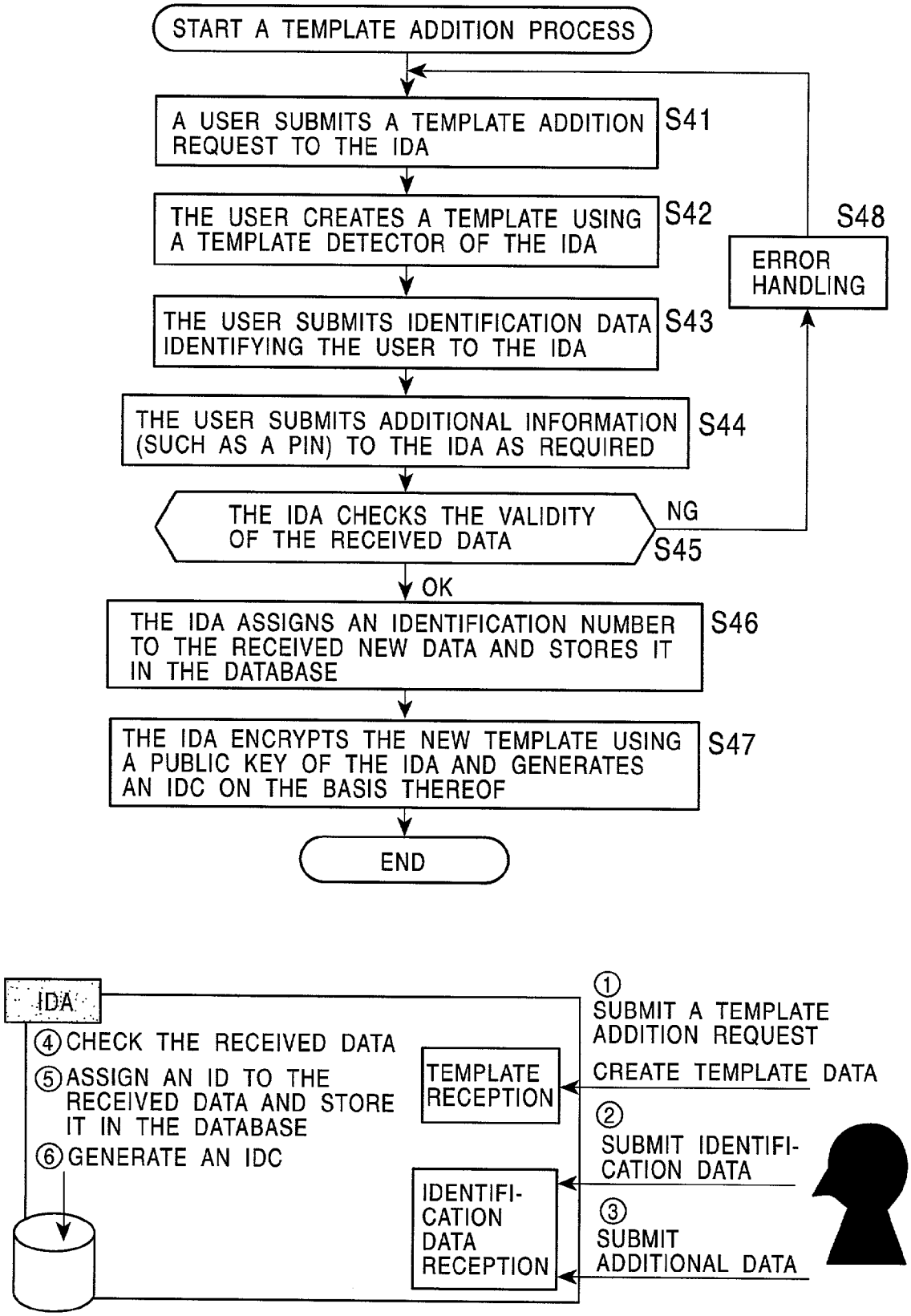

START A TEMPLATE CHANGING PROCESS
A USER SUBMITS A TEMPLATE CHANGE REQUEST TO THE IDA
S31
THE USER CREATES A TEMPLATE USING A TEMPLATE DETECTOR OF THE IDA
S32
THE USER SUBMITS IDENTIFICATION DATA IDENTIFYING THE USER TO THE IDA
S33
THE USER SUBMITS ADDITIONAL INFORMATION (SUCH AS A PIN) TO THE IDA AS REQUIRED
S34
THE IDA CHECKS THE VALIDITY OF THE RECEIVED DATA
NG
S35
OK
THE IDA DELETES A REGISTERED TEMPLATE
S36
THE IDA DELETES THE IDC OF THE USER AND DESCRIBES, IN THE INVALIDATED IDC LIST, THAT THE IDC HAS BEEN INVALIDATED
S37
THE IDA ASSIGNS AN INDENTIFICATION NUMBER TO THE RECEIVED NEW DATA AND STORES IT IN THE DATABASE
S38
THE IDA ENCRYPTS THE NEW TEMPLATE USING A PUBLIC KEY OF THE IDA AND GENERATES AN IDC ON THE BASIS THEROEOF
S39
END
S40
ERROR HANDLING
IDA
④ CHECK THE RECEIVED DATA
⑤ DELETE THE PERSONAL DATA
⑥ DESCRIBE THE INVALIDATION IN THE INVALIDATED IDC LIST
⑦ ASSIGN AN ID TO THE RECEIVED NEW DATA AND STORES IT IN THE DATABASE
⑧ GENERATE AN IDC
TEMPLATE RECEPTION
IDENTIFI-CATION DATA RECEPTION
① SUBMIT A TEMPLATE CHANGE REQUEST AND CREATE TEMPLATE DATA
② SUBMIT IDENTIFI-CATION DATA
③ SUBMIT ADDITIONAL DATA

FIG. 12


START A TEMPLATE ADDITION PROCESS
A USER SUBMITS A TEMPLATE ADDITION REQUEST TO THE IDA
S41
THE USER CREATES A TEMPLATE USING A TEMPLATE DETECTOR OF THE IDA
S42
THE USER SUBMITS IDENTIFICATION DATA IDENTIFYING THE USER TO THE IDA
S43
THE USER SUBMITS ADDITIONAL INFORMATION (SUCH AS A PIN) TO THE IDA AS REQUIRED
S44
THE IDA CHECKS THE VALIDITY OF THE RECEIVED DATA
NG
S45
S48
ERROR HANDLING
OK
THE IDA ASSIGNS AN IDENTIFICATION NUMBER TO THE RECEIVED NEW DATA AND STORES IT IN THE DATABASE
S46
THE IDA ENCRYPTS THE NEW TEMPLATE USING A PUBLIC KEY OF THE IDA AND GENERATES AN IDC ON THE BASIS THEREOF
S47
END

IDA
④CHECK THE RECEIVED DATA
⑤ASSIGN AN ID TO THE RECEIVED DATA AND STORE IT IN THE DATABASE
⑥GENERATE AN IDC
TEMPLATE RECEPTION
IDENTIFI-CATION DATA RECEPTION
①SUBMIT A TEMPLATE ADDITION REQUEST
CREATE TEMPLATE DATA
②SUBMIT IDENTIFI-CATION DATA
③SUBMIT ADDITIONAL DATA

FIG. 13

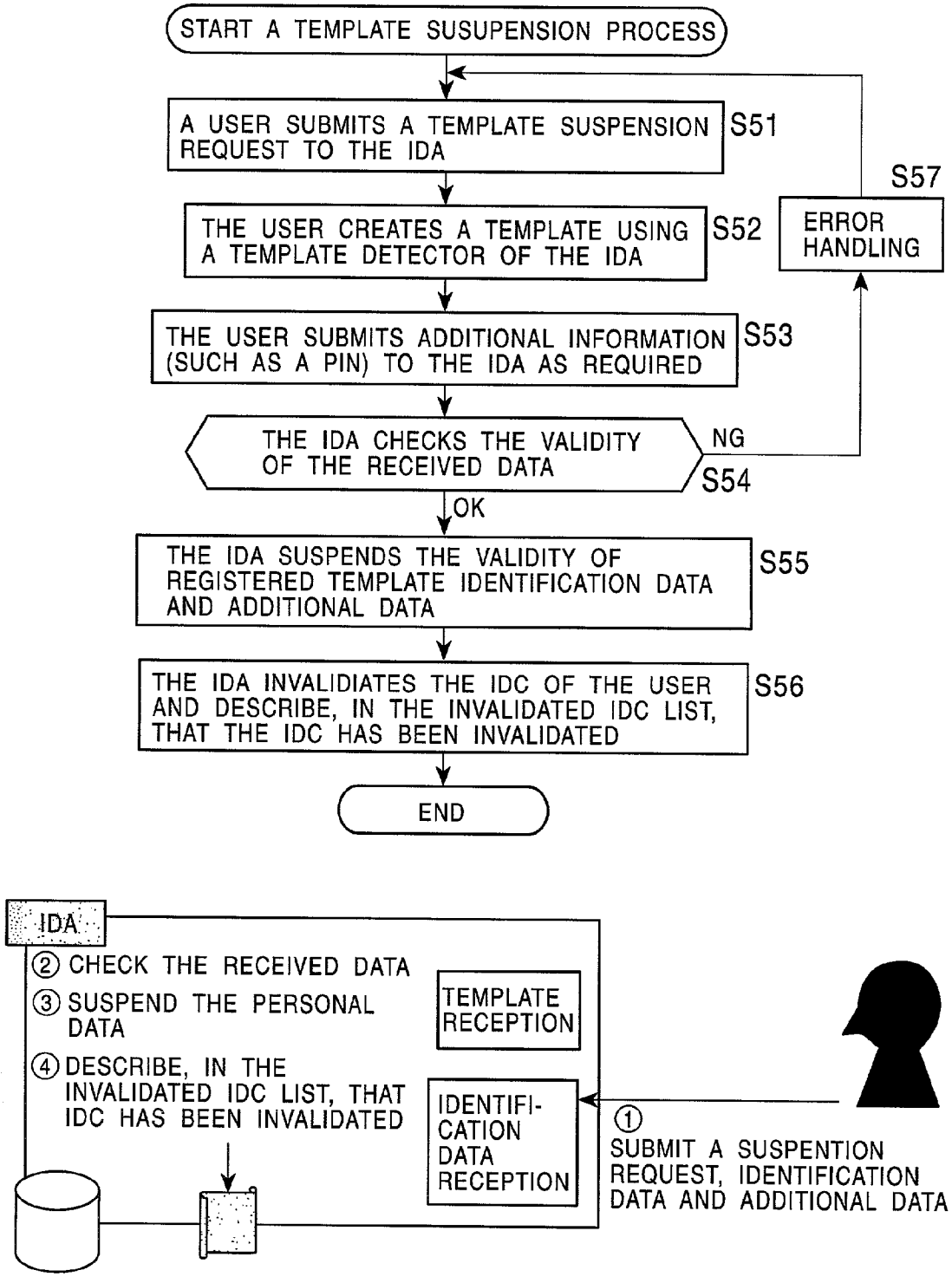

START A TEMPLATE SUSUPENSION PROCESS
A USER SUBMITS A TEMPLATE SUSPENSION REQUEST TO THE IDA
S51
THE USER CREATES A TEMPLATE USING A TEMPLATE DETECTOR OF THE IDA
S52
THE USER SUBMITS ADDITIONAL INFORMATION (SUCH AS A PIN) TO THE IDA AS REQUIRED
S53
THE IDA CHECKS THE VALIDITY OF THE RECEIVED DATA
NG
S54
OK
THE IDA SUSPENDS THE VALIDITY OF REGISTERED TEMPLATE IDENTIFICATION DATA AND ADDITIONAL DATA
S55
THE IDA INVALIDIATES THE IDC OF THE USER AND DESCRIBE, IN THE INVALIDATED IDC LIST, THAT THE IDC HAS BEEN INVALIDATED
S56
END
S57
ERROR HANDLING
IDA
② CHECK THE RECEIVED DATA
③ SUSPEND THE PERSONAL DATA
④ DESCRIBE, IN THE INVALIDATED IDC LIST, THAT IDC HAS BEEN INVALIDATED
TEMPLATE RECEPTION
IDENTIFI-CATION DATA RECEPTION
① SUBMIT A SUSPENTION REQUEST, IDENTIFICATION DATA AND ADDITIONAL DATA

FIG. 14

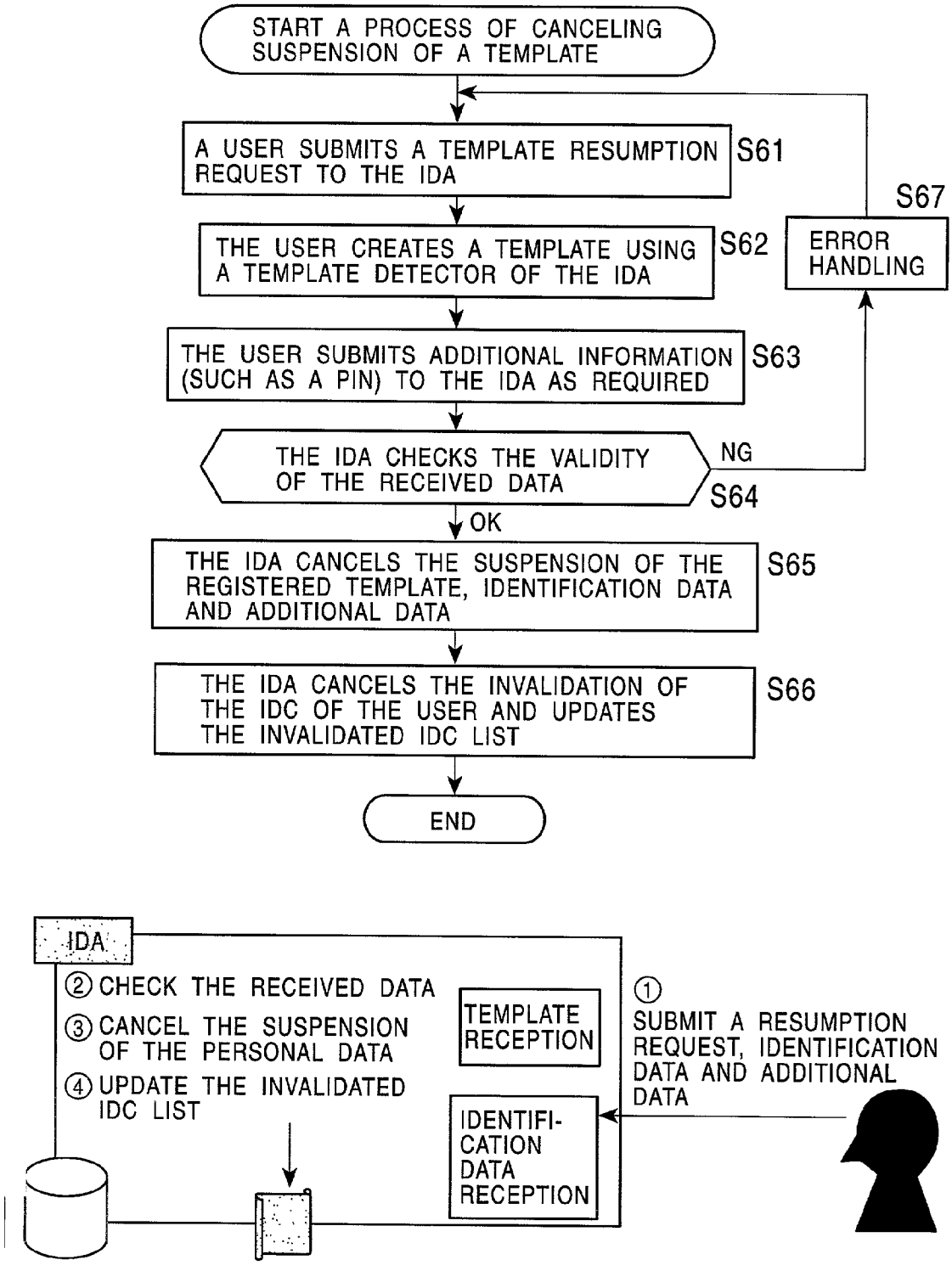

START A PROCESS OF CANCELING SUSPENSION OF A TEMPLATE
A USER SUBMITS A TEMPLATE RESUMPTION REQUEST TO THE IDA
S61
THE USER CREATES A TEMPLATE USING A TEMPLATE DETECTOR OF THE IDA
S62
THE USER SUBMITS ADDITIONAL INFORMATION (SUCH AS A PIN) TO THE IDA AS REQUIRED
S63
THE IDA CHECKS THE VALIDITY OF THE RECEIVED DATA
NG
S64
OK
THE IDA CANCELS THE SUSPENSION OF THE REGISTERED TEMPLATE, IDENTIFICATION DATA AND ADDITIONAL DATA
S65
THE IDA CANCELS THE INVALIDATION OF THE IDC OF THE USER AND UPDATES THE INVALIDATED IDC LIST
S66
END
S67
ERROR HANDLING
IDA
② CHECK THE RECEIVED DATA
③ CANCEL THE SUSPENSION OF THE PERSONAL DATA
④ UPDATE THE INVALIDATED IDC LIST
TEMPLATE RECEPTION
IDENTIFI-CATION DATA RECEPTION
① SUBMIT A RESUMPTION REQUEST, IDENTIFICATION DATA AND ADDITIONAL DATA

FIG. 15

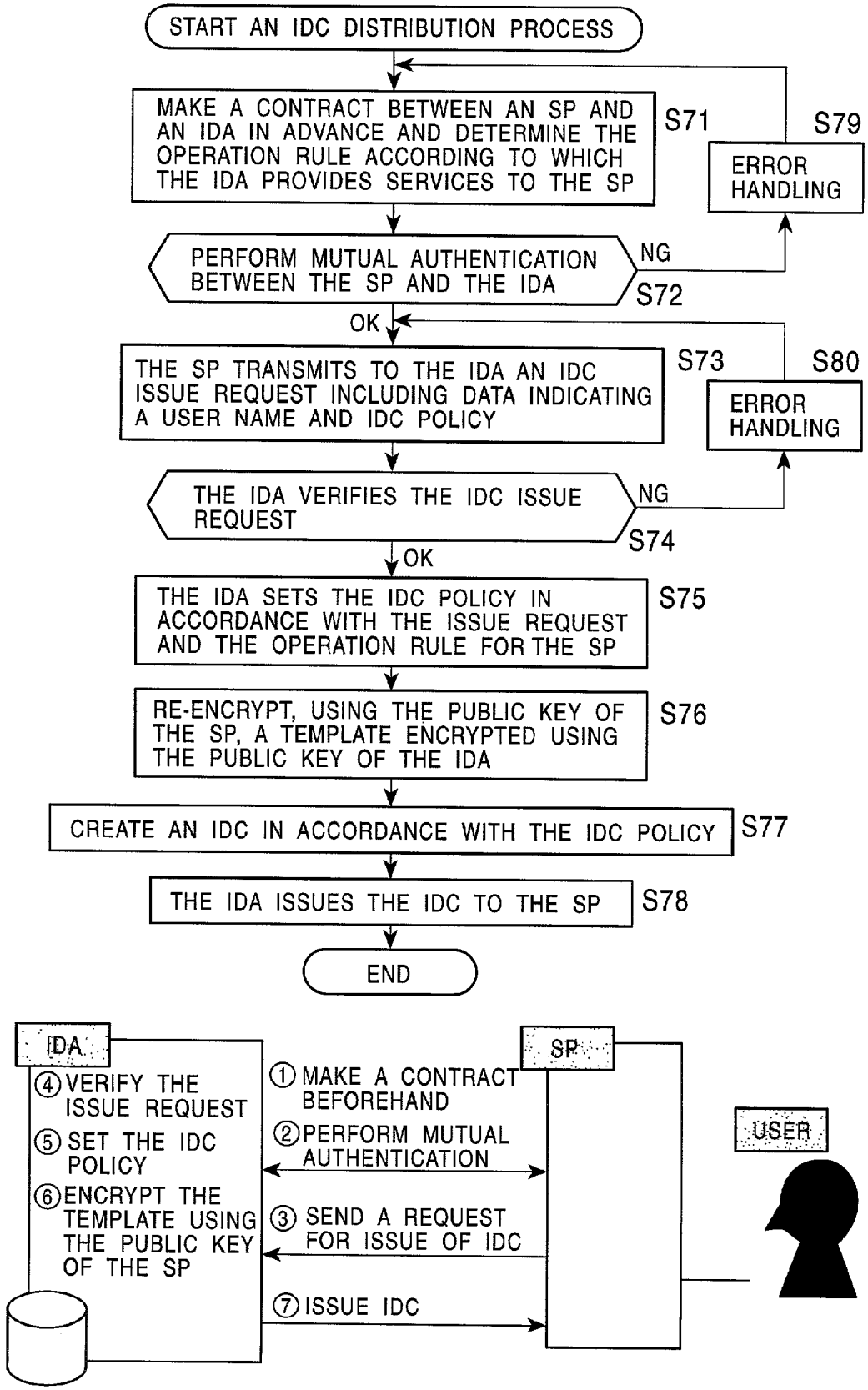

START AN IDC DISTRIBUTION PROCESS
MAKE A CONTRACT BETWEEN AN SP AND AN IDA IN ADVANCE AND DETERMINE THE OPERATION RULE ACCORDING TO WHICH THE IDA PROVIDES SERVICES TO THE SP
S71
S79
ERROR HANDLING
PERFORM MUTUAL AUTHENTICATION BETWEEN THE SP AND THE IDA
NG
S72
OK
THE SP TRANSMITS TO THE IDA AN IDC ISSUE REQUEST INCLUDING DATA INDICATING A USER NAME AND IDC POLICY
S73
S80
ERROR HANDLING
THE IDA VERIFIES THE IDC ISSUE REQUEST
NG
S74
OK
THE IDA SETS THE IDC POLICY IN ACCORDANCE WITH THE ISSUE REQUEST AND THE OPERATION RULE FOR THE SP
S75
RE-ENCRYPT, USING THE PUBLIC KEY OF THE SP, A TEMPLATE ENCRYPTED USING THE PUBLIC KEY OF THE IDA
S76
CREATE AN IDC IN ACCORDANCE WITH THE IDC POLICY
S77
THE IDA ISSUES THE IDC TO THE SP
S78
END
IDA
④ VERIFY THE ISSUE REQUEST
⑤ SET THE IDC POLICY
⑥ ENCRYPT THE TEMPLATE USING THE PUBLIC KEY OF THE SP
① MAKE A CONTRACT BEFOREHAND
② PERFORM MUTUAL AUTHENTICATION
③ SEND A REQUEST FOR ISSUE OF IDC
⑦ ISSUE IDC
SP
USER

FIG. 16

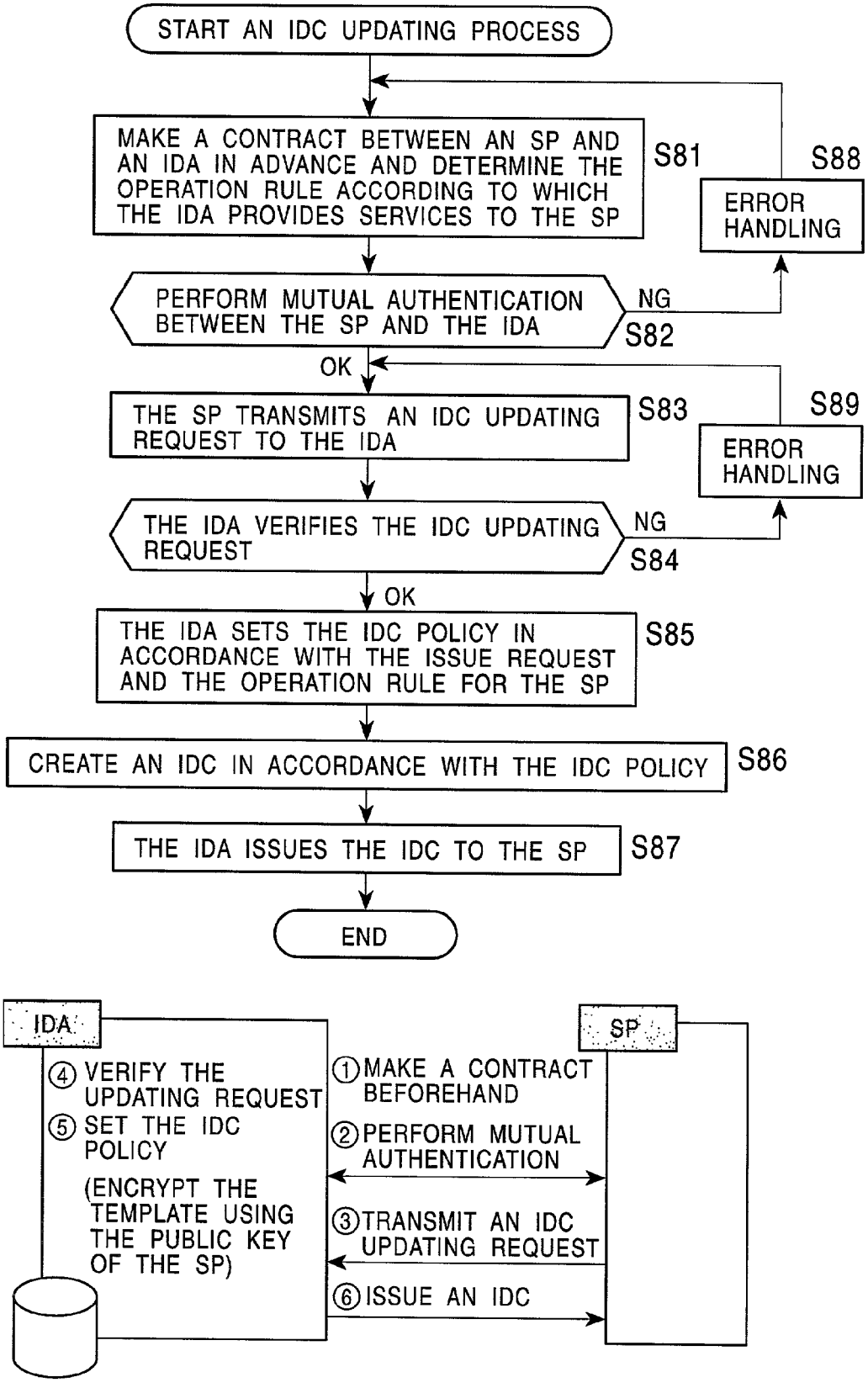
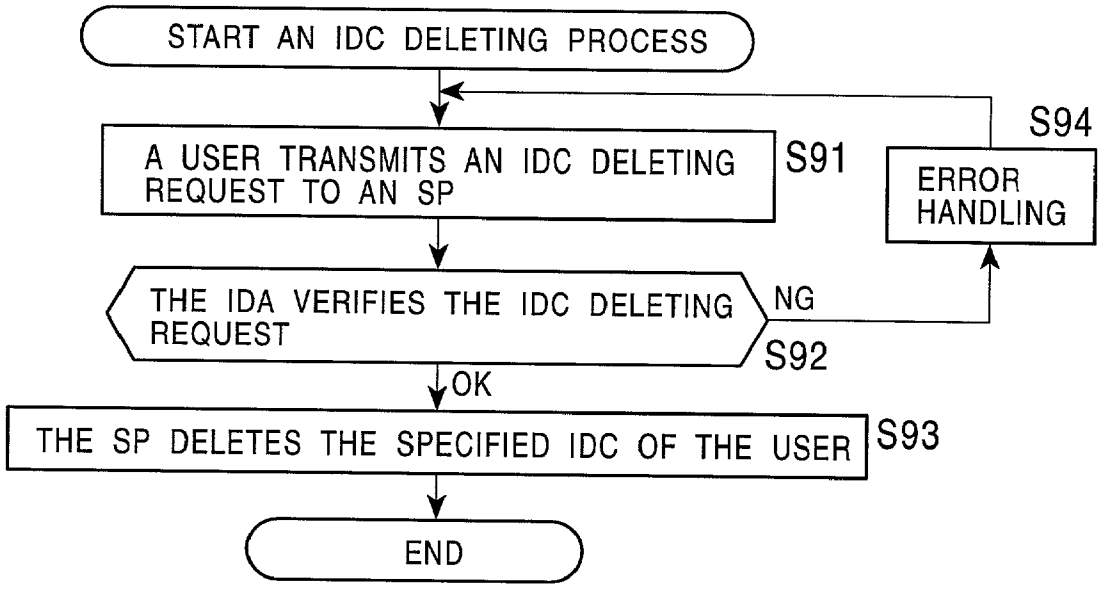

START AN IDC UPDATING PROCESS
MAKE A CONTRACT BETWEEN AN SP AND AN IDA IN ADVANCE AND DETERMINE THE OPERATION RULE ACCORDING TO WHICH THE IDA PROVIDES SERVICES TO THE SP
S81
S88
ERROR HANDLING
PERFORM MUTUAL AUTHENTICATION BETWEEN THE SP AND THE IDA
NG
S82
OK
THE SP TRANSMITS AN IDC UPDATING REQUEST TO THE IDA
S83
S89
ERROR HANDLING
THE IDA VERIFIES THE IDC UPDATING REQUEST
NG
S84
OK
THE IDA SETS THE IDC POLICY IN ACCORDANCE WITH THE ISSUE REQUEST AND THE OPERATION RULE FOR THE SP
S85
CREATE AN IDC IN ACCORDANCE WITH THE IDC POLICY
S86
THE IDA ISSUES THE IDC TO THE SP
S87
END
IDA
SP
④ VERIFY THE UPDATING REQUEST
⑤ SET THE IDC POLICY
(ENCRYPT THE TEMPLATE USING THE PUBLIC KEY OF THE SP)
①MAKE A CONTRACT BEFOREHAND
②PERFORM MUTUAL AUTHENTICATION
③TRANSMIT AN IDC UPDATING REQUEST
⑥ISSUE AN IDC

FIG. 17


START AN IDC DELETING PROCESS
A USER TRANSMITS AN IDC DELETING REQUEST TO AN SP
S91
S94
ERROR HANDLING
THE IDA VERIFIES THE IDC DELETING REQUEST
NG
S92
OK
THE SP DELETES THE SPECIFIED IDC OF THE USER
S93
END

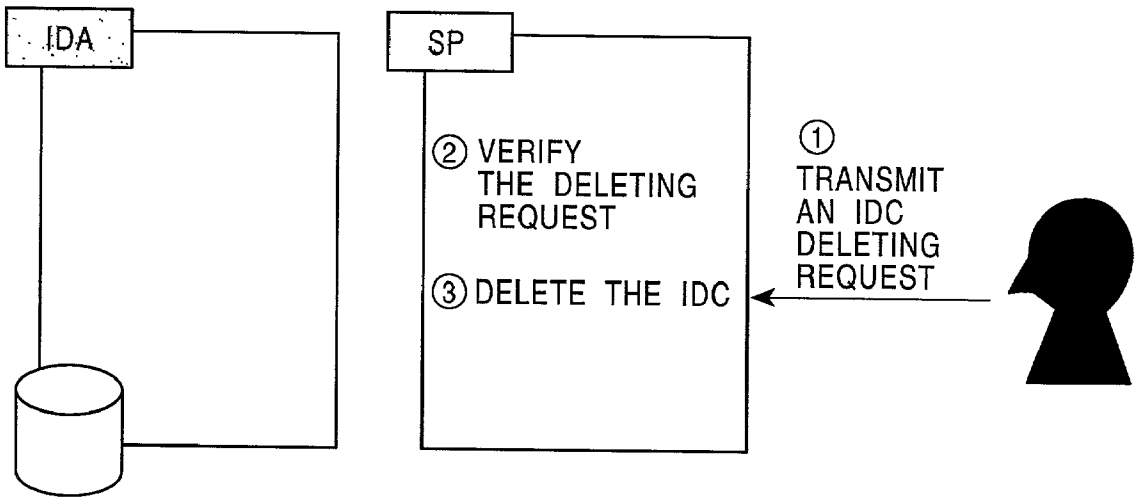

IDA
SP
② VERIFY THE DELETING REQUEST
③ DELETE THE IDC
① TRANSMIT AN IDC DELETING REQUEST

FIG. 18

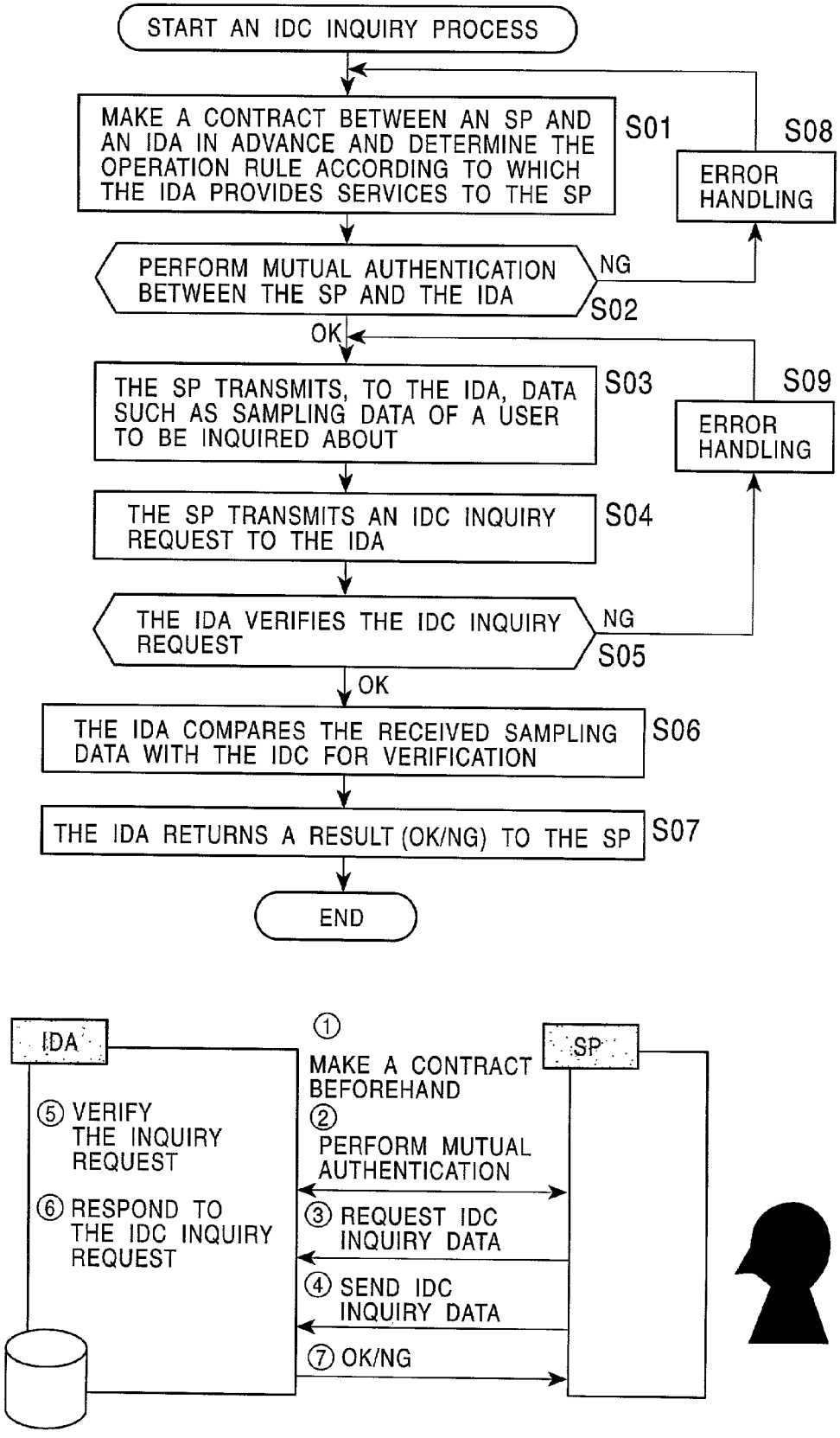

START AN IDC INQUIRY PROCESS
MAKE A CONTRACT BETWEEN AN SP AND AN IDA IN ADVANCE AND DETERMINE THE OPERATION RULE ACCORDING TO WHICH THE IDA PROVIDES SERVICES TO THE SP
S01
S08
ERROR HANDLING
PERFORM MUTUAL AUTHENTICATION BETWEEN THE SP AND THE IDA
NG
S02
OK
THE SP TRANSMITS, TO THE IDA, DATA SUCH AS SAMPLING DATA OF A USER TO BE INQUIRED ABOUT
S03
S09
ERROR HANDLING
THE SP TRANSMITS AN IDC INQUIRY REQUEST TO THE IDA
S04
THE IDA VERIFIES THE IDC INQUIRY REQUEST
NG
S05
OK
THE IDA COMPARES THE RECEIVED SAMPLING DATA WITH THE IDC FOR VERIFICATION
S06
THE IDA RETURNS A RESULT (OK/NG) TO THE SP
S07
END
IDA
SP
① MAKE A CONTRACT BEFOREHAND
② PERFORM MUTUAL AUTHENTICATION
③ REQUEST IDC INQUIRY DATA
④ SEND IDC INQUIRY DATA
⑤ VERIFY THE INQUIRY REQUEST
⑥ RESPOND TO THE IDC INQUIRY REQUEST
⑦ OK/NG

FIG. 19

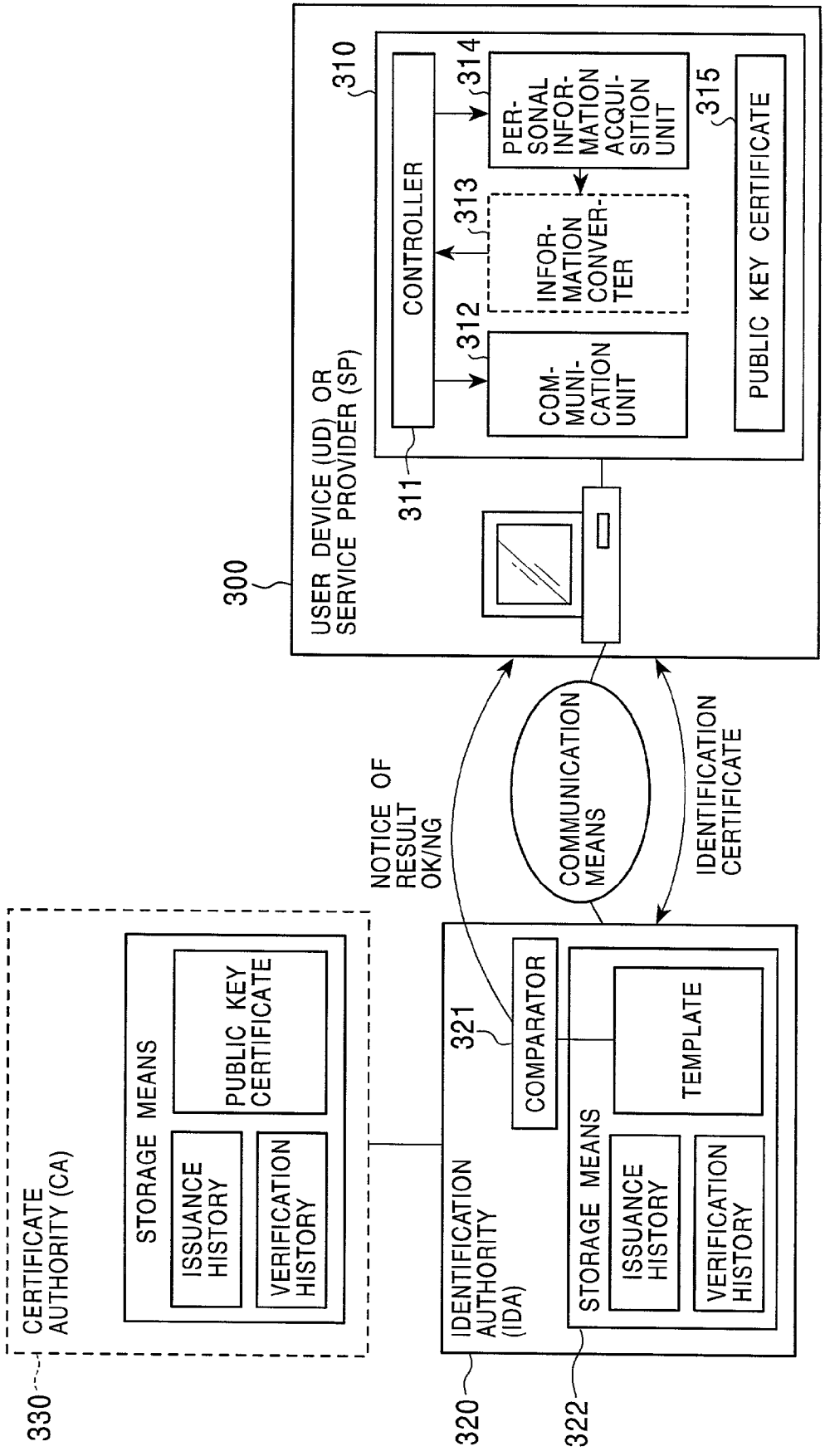

USER DEVICE (UD) OR SERVICE PROVIDER (SP)
300
310
CONTROLLER
311
312
313
314
315
COM-MUNI-CATION UNIT
INFOR-MATION CONVER-TER
PER-SONAL INFOR-MATION ACQUI-SITION UNIT
PUBLIC KEY CERTIFICATE
NOTICE OF RESULT OK/NG
COMMUNICATION MEANS
IDENTIFICATION CERTIFICATE
IDENTIFICATION AUTHORITY (IDA)
320
321
322
COMPARATOR
TEMPLATE
STORAGE MEANS
ISSUANCE HISTORY
VERIFICATION HISTORY
CERTIFICATE AUTHORITY (CA)
330
STORAGE MEANS
PUBLIC KEY CERTIFICATE
ISSUANCE HISTORY
VERIFICATION HISTORY

FIG. 20

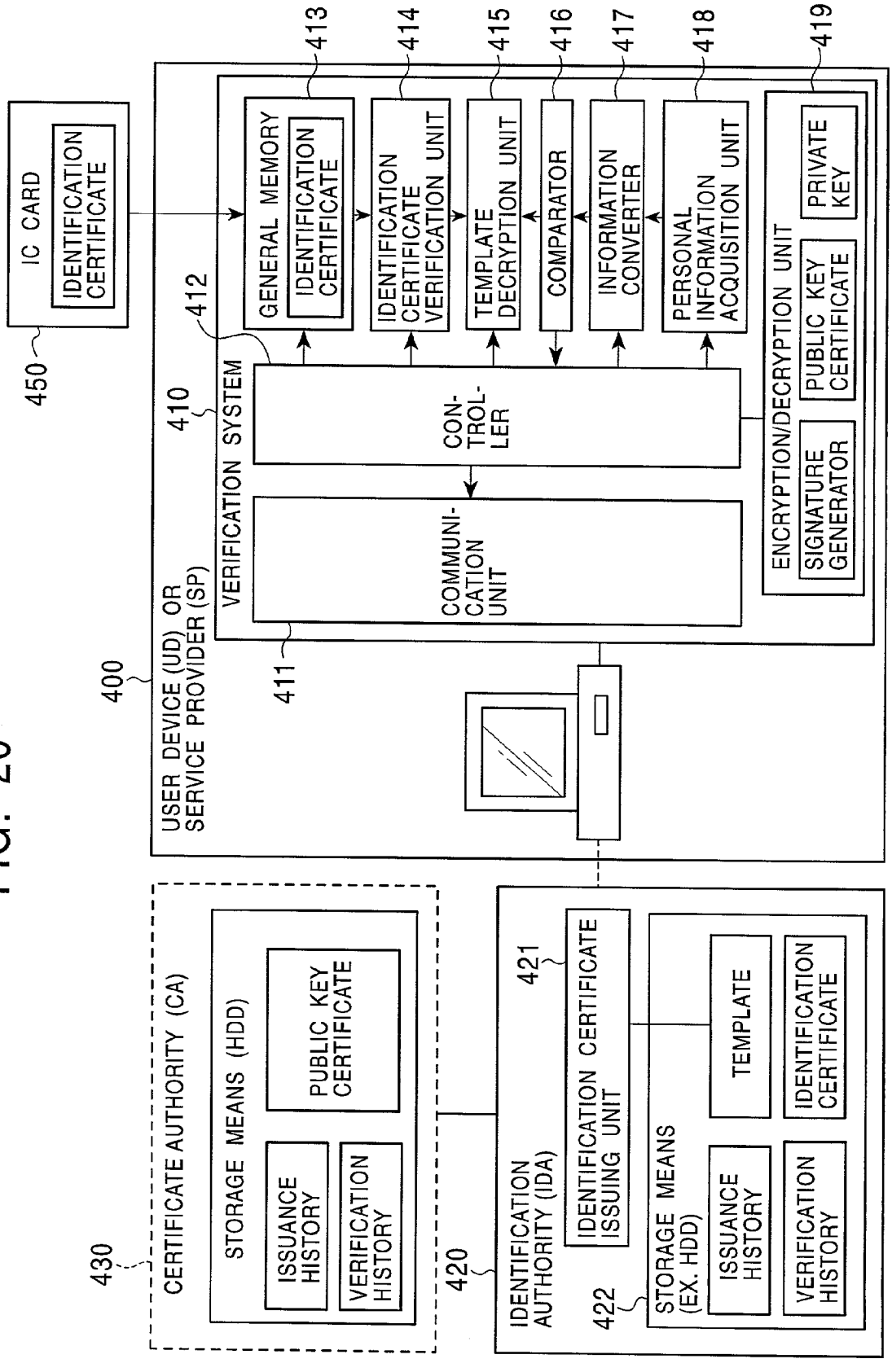

IC CARD
IDENTIFICATION CERTIFICATE
450
USER DEVICE (UD) OR SERVICE PROVIDER (SP)
400
VERIFICATION SYSTEM
410
412
411
GENERAL MEMORY
IDENTIFICATION CERTIFICATE
413
IDENTIFICATION CERTIFICATE VERIFICATION UNIT
414
TEMPLATE DECRYPTION UNIT
415
COMPARATOR
416
INFORMATION CONVERTER
417
PERSONAL INFORMATION ACQUISITION UNIT
418
ENCRYPTION/DECRYPTION UNIT
419
PRIVATE KEY
PUBLIC KEY CERTIFICATE
SIGNATURE GENERATOR
CON-TROL-LER
COMMUNI-CATION UNIT
CERTIFICATE AUTHORITY (CA)
430
STORAGE MEANS (HDD)
PUBLIC KEY CERTIFICATE
ISSUANCE HISTORY
VERIFICATION HISTORY
IDENTIFICATION AUTHORITY (IDA)
420
421
IDENTIFICATION CERTIFICATE ISSUING UNIT
422
STORAGE MEANS (EX. HDD)
TEMPLATE
IDENTIFICATION CERTIFICATE
ISSUANCE HISTORY
VERIFICATION HISTORY

FIG. 21A

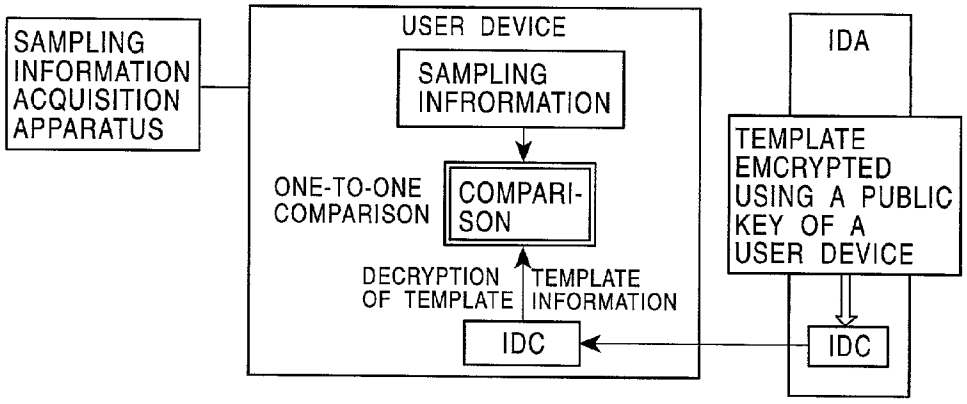


FIG. 21B

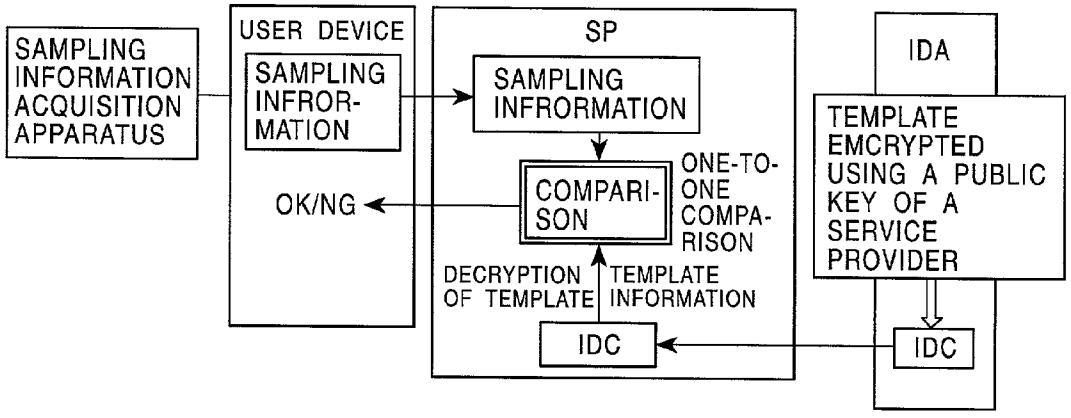


FIG. 21C

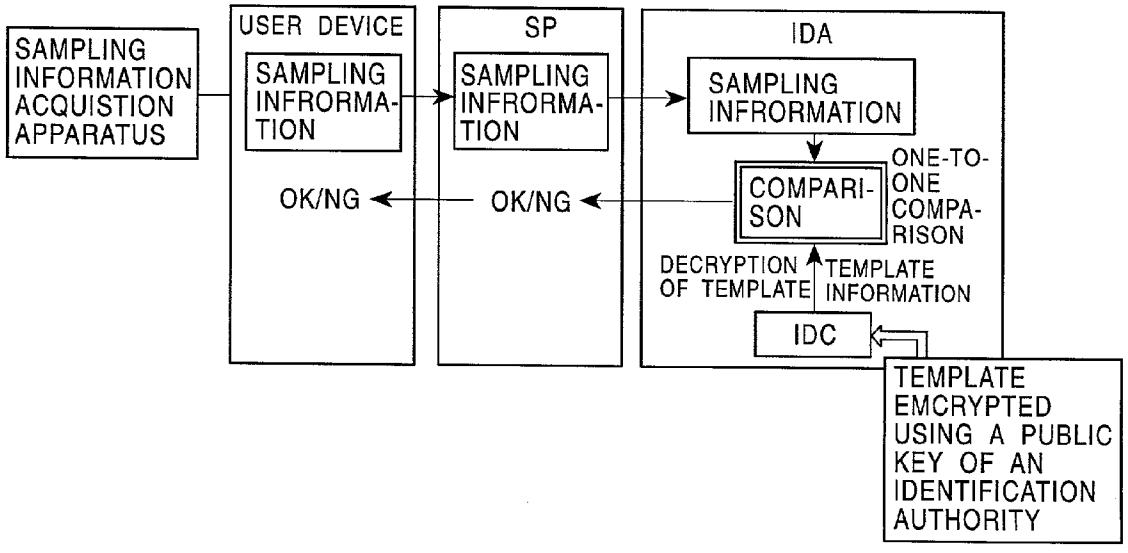
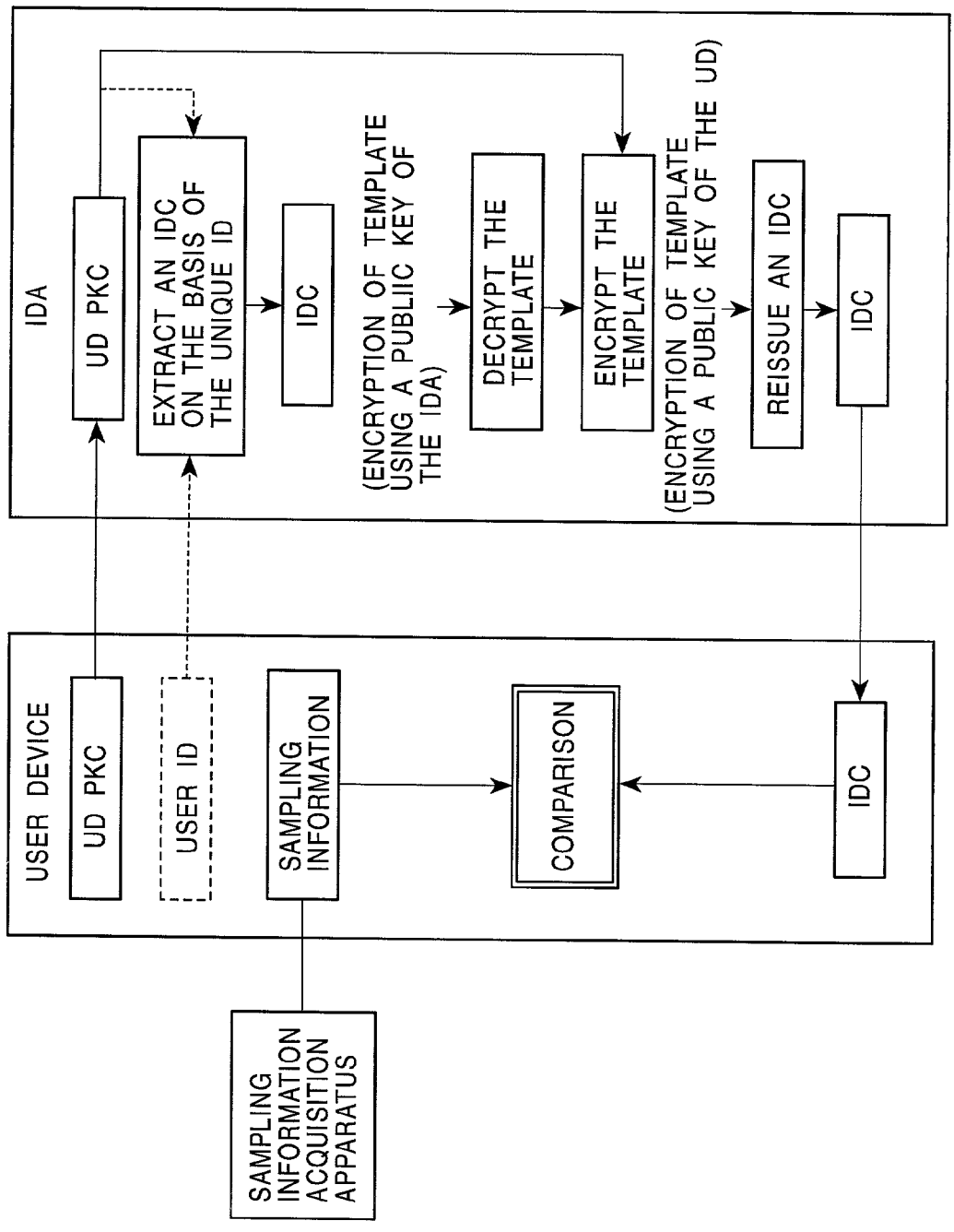


FIG. 22


IDA
UD PKC
EXTRACT AN IDC ON THE BASIS OF THE UNIQUE ID
IDC
(ENCRYPTION OF TEMPLATE USING A PUBLIIC KEY OF THE IDA)
DECRYPT THE TEMPLATE
ENCRYPT THE TEMPLATE
(ENCRYPTION OF TEMPLATE USING A PUBLIC KEY OF THE UD)
REISSUE AN IDC
IDC
USER DEVICE
UD PKC
USER ID
SAMPLING INFORMATION
COMPARISON
IDC
SAMPLING INFORMATION ACQUISITION APPARATUS

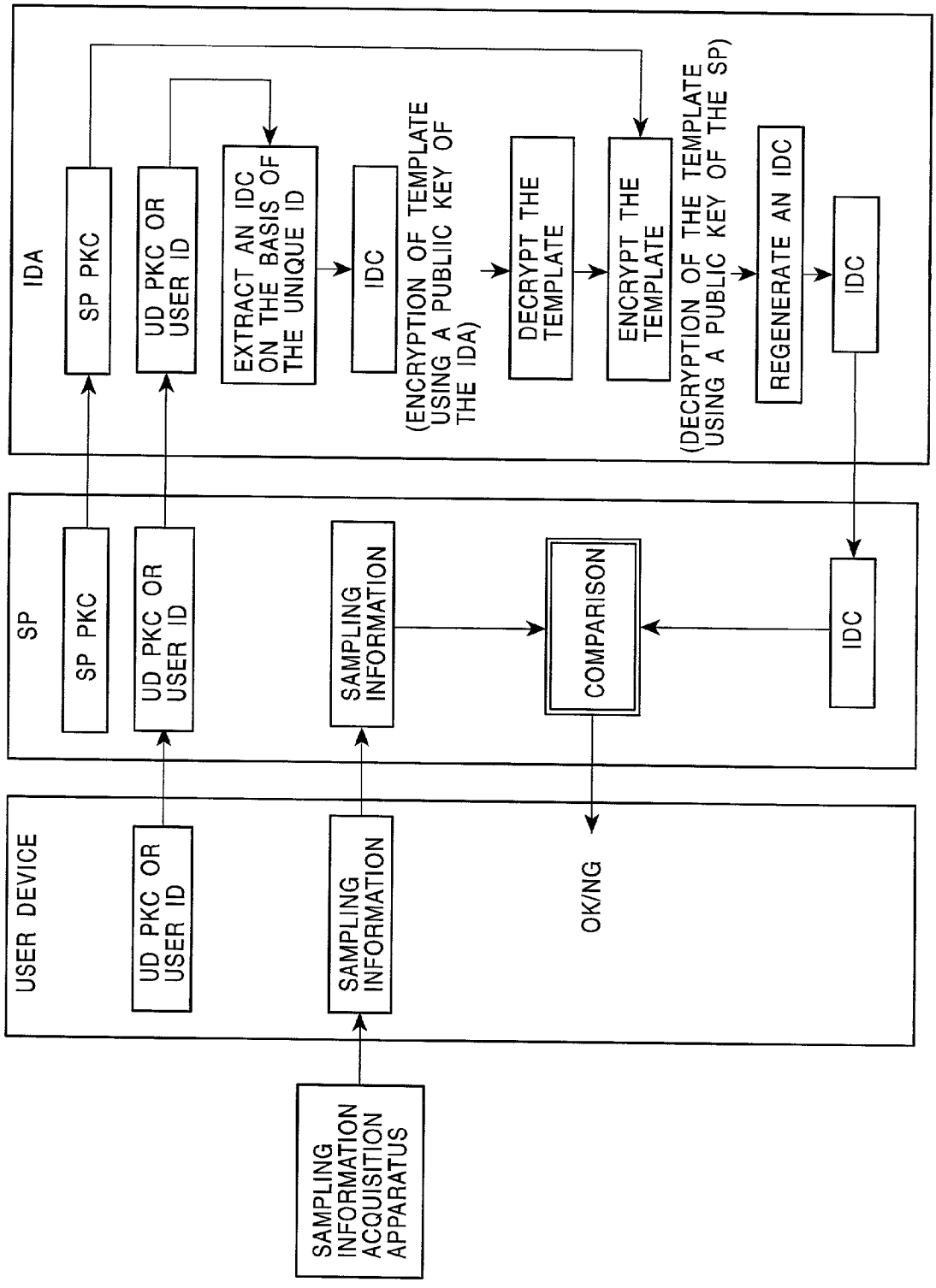

IDA
SP PKC
UD PKC OR USER ID
EXTRACT AN IDC ON THE BASIS OF THE UNIQUE ID
IDC
(ENCRYPTION OF TEMPLATE USING A PUBLIIC KEY OF THE IDA)
DECRYPT THE TEMPLATE
ENCRYPT THE TEMPLATE
(DECRYPTION OF THE TEMPLATE USING A PUBLIC KEY OF THE SP)
REGENERATE AN IDC
IDC
SP
SP PKC
UD PKC OR USER ID
SAMPLING INFORMATION
COMPARISON
IDC
USER DEVICE
UD PKC OR USER ID
SAMPLING INFORMATION
OK/NG
SAMPLING INFORMATION ACQUISITION APPARATUS

FIG. 23

FIG. 24

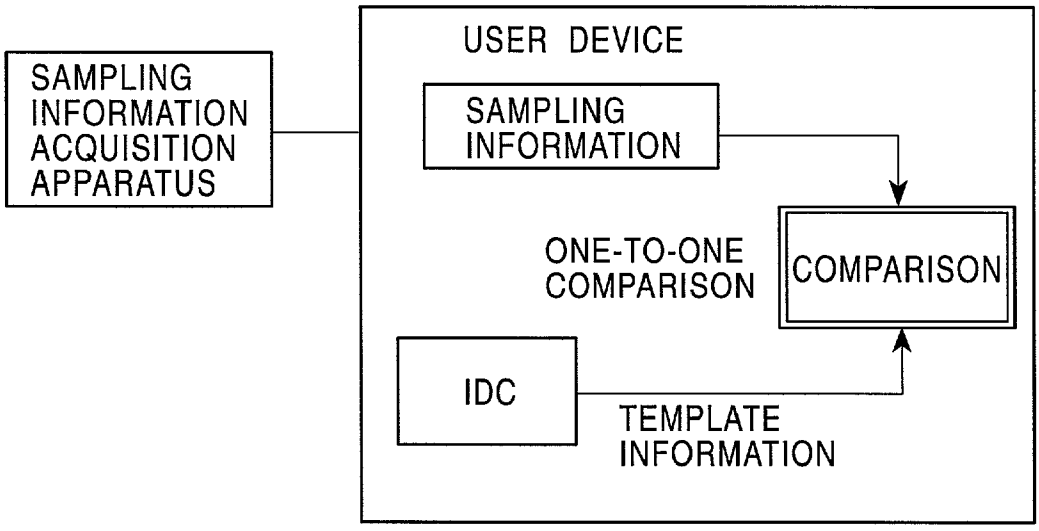

SAMPLING INFORMATION ACQUISITION APPARATUS
USER DEVICE
SAMPLING INFORMATION
ONE-TO-ONE COMPARISON
COMPARISON
IDC
TEMPLATE INFORMATION

FIG. 25

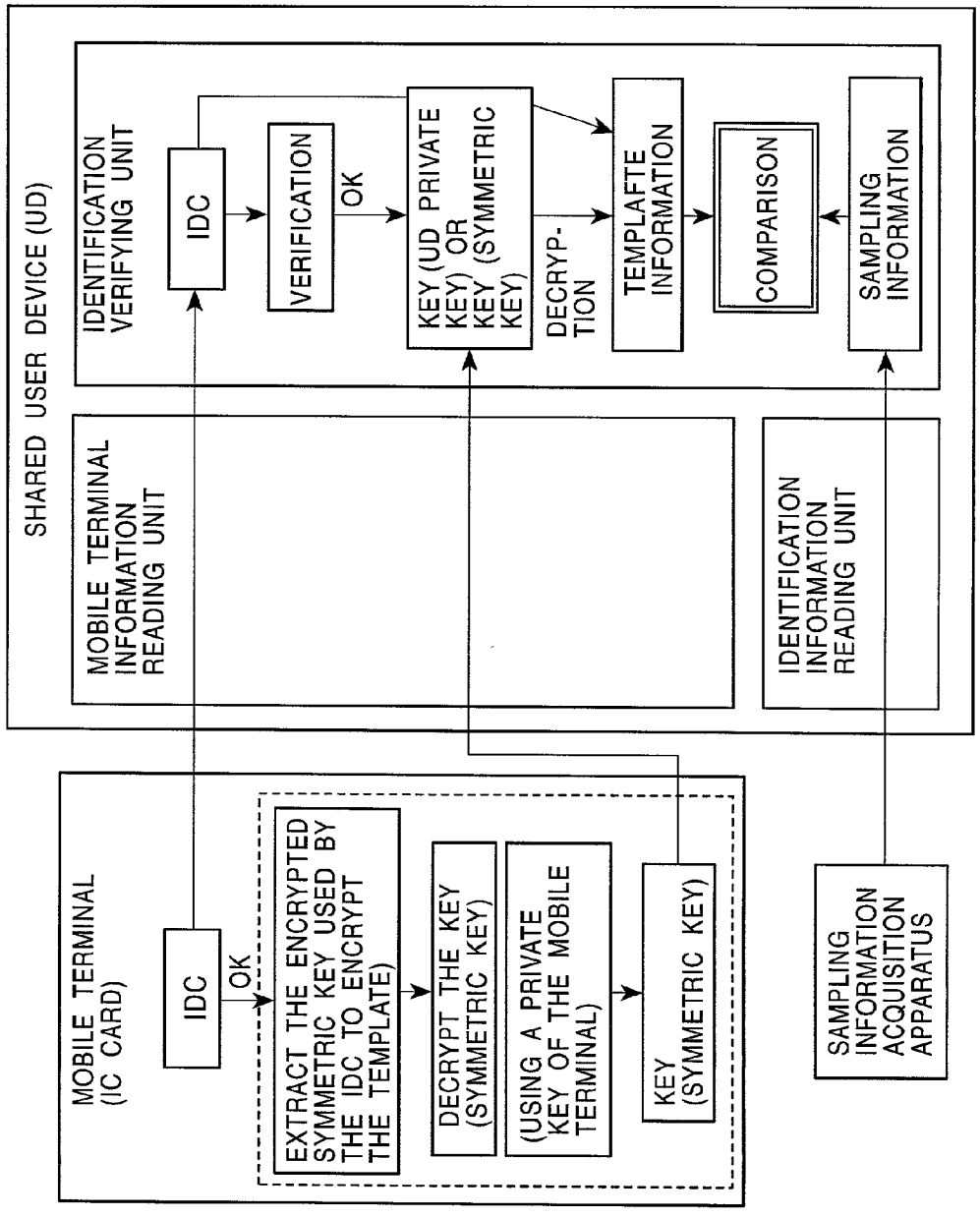

SHARED USER DEVICE (UD)
IDENTIFICATION VERIFYING UNIT
IDC
VERIFICATION
OK
KEY (UD PRIVATE KEY) OR KEY (SYMMETRIC KEY)
DECRYP-TION
TEMPLAFTE INFORMATION
COMPARISON
SAMPLING INFORMATION
MOBILE TERMINAL INFORMATION READING UNIT
IDENTIFICATION INFORMATION READING UNIT
MOBILE TERMINAL (IC CARD)
IDC
OK
EXTRACT THE ENCRYPTED SYMMETRIC KEY USED BY THE IDC TO ENCRYPT THE TEMPLATE)
DECRYPT THE KEY (SYMMETRIC KEY)
(USING A PRIVATE KEY OF THE MOBILE TERMINAL)
KEY (SYMMETRIC KEY)
SAMPLING INFORMATION ACQUISITION APPARATUS

FIG. 26

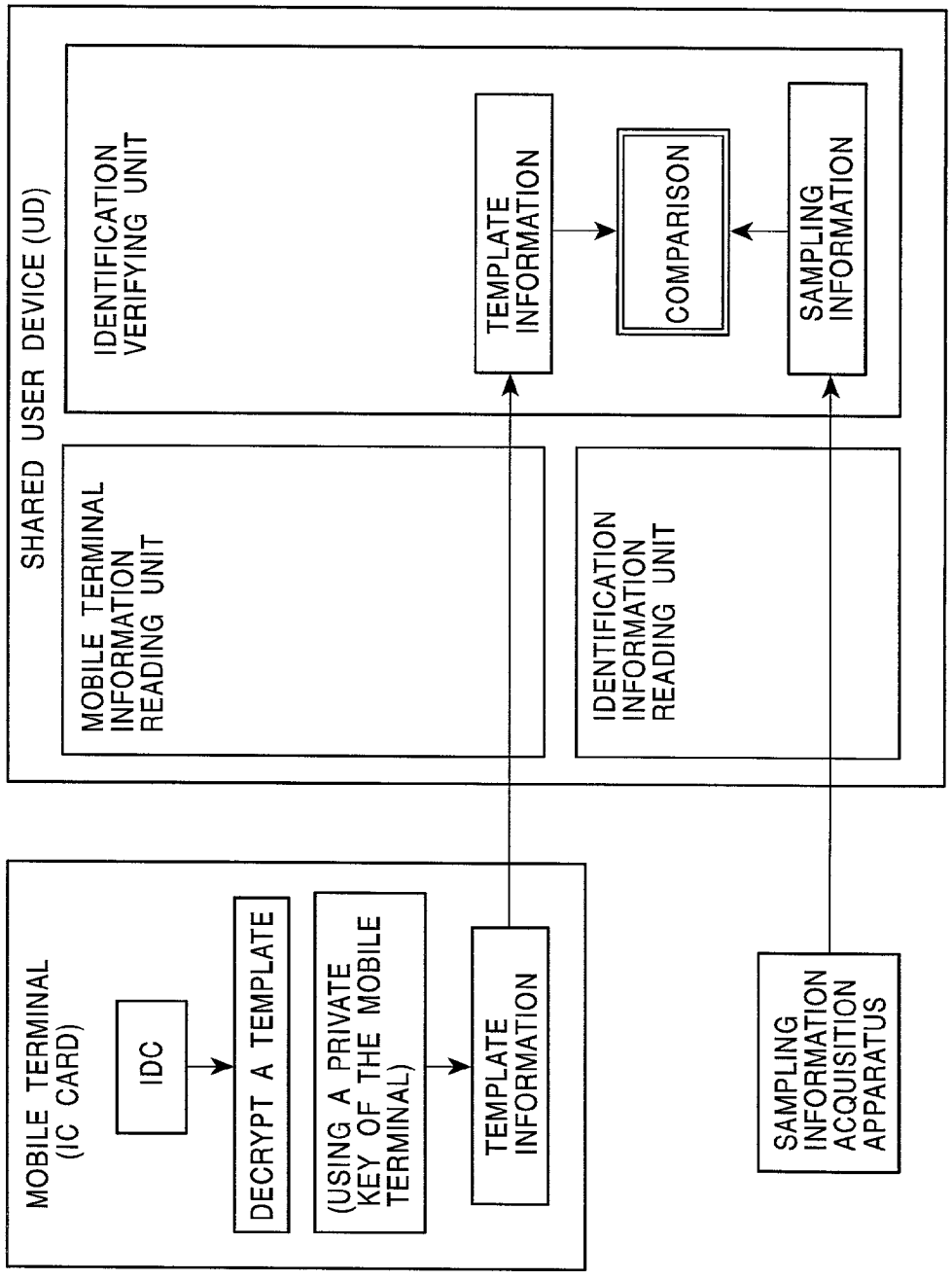

SHARED USER DEVICE (UD)
IDENTIFICATION VERIFYING UNIT
TEMPLATE INFORMATION
COMPARISON
SAMPLING INFORMATION
MOBILE TERMINAL INFORMATION READING UNIT
IDENTIFICATION INFORMATION READING UNIT
MOBILE TERMINAL (IC CARD)
IDC
DECRYPT A TEMPLATE
(USING A PRIVATE KEY OF THE MOBILE TERMINAL)
TEMPLATE INFORMATION
SAMPLING INFORMATION ACQUISITION APPARATUS

FIG. 27

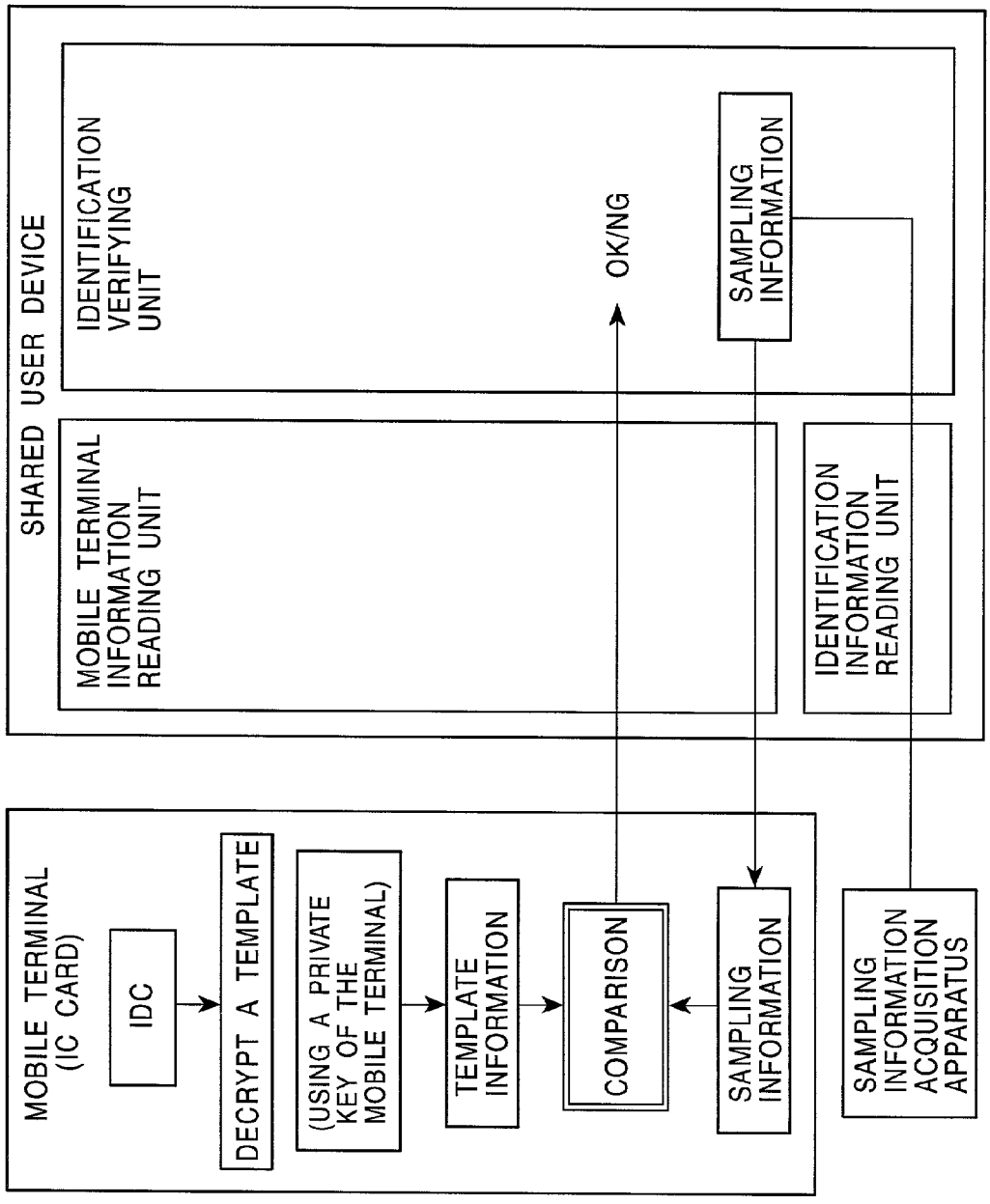

SHARED USER DEVICE
IDENTIFICATION VERIFYING UNIT
MOBILE TERMINAL INFORMATION READING UNIT
IDENTIFICATION INFORMATION READING UNIT
OK/NG
SAMPLING INFORMATION
MOBILE TERMINAL (IC CARD)
IDC
DECRYPT A TEMPLATE
(USING A PRIVATE KEY OF THE MOBILE TERMINAL)
TEMPLATE INFORMATION
COMPARISON
SAMPLING INFORMATION
SAMPLING INFORMATION ACQUISITION APPARATUS

FIG. 28

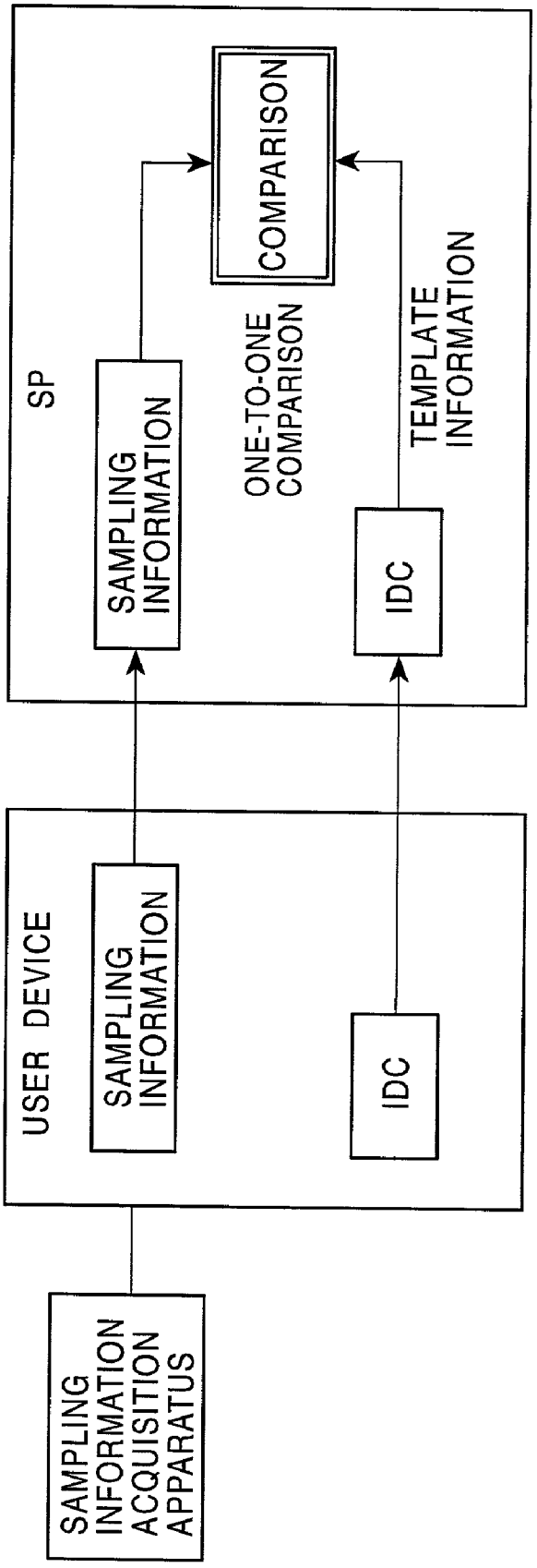

SAMPLING INFORMATION ACQUISITION APPARATUS
USER DEVICE
SAMPLING INFORMATION
IDC
SP
SAMPLING INFORMATION
ONE-TO-ONE COMPARISON
IDC
TEMPLATE INFORMATION
COMPARISON

FIG. 29

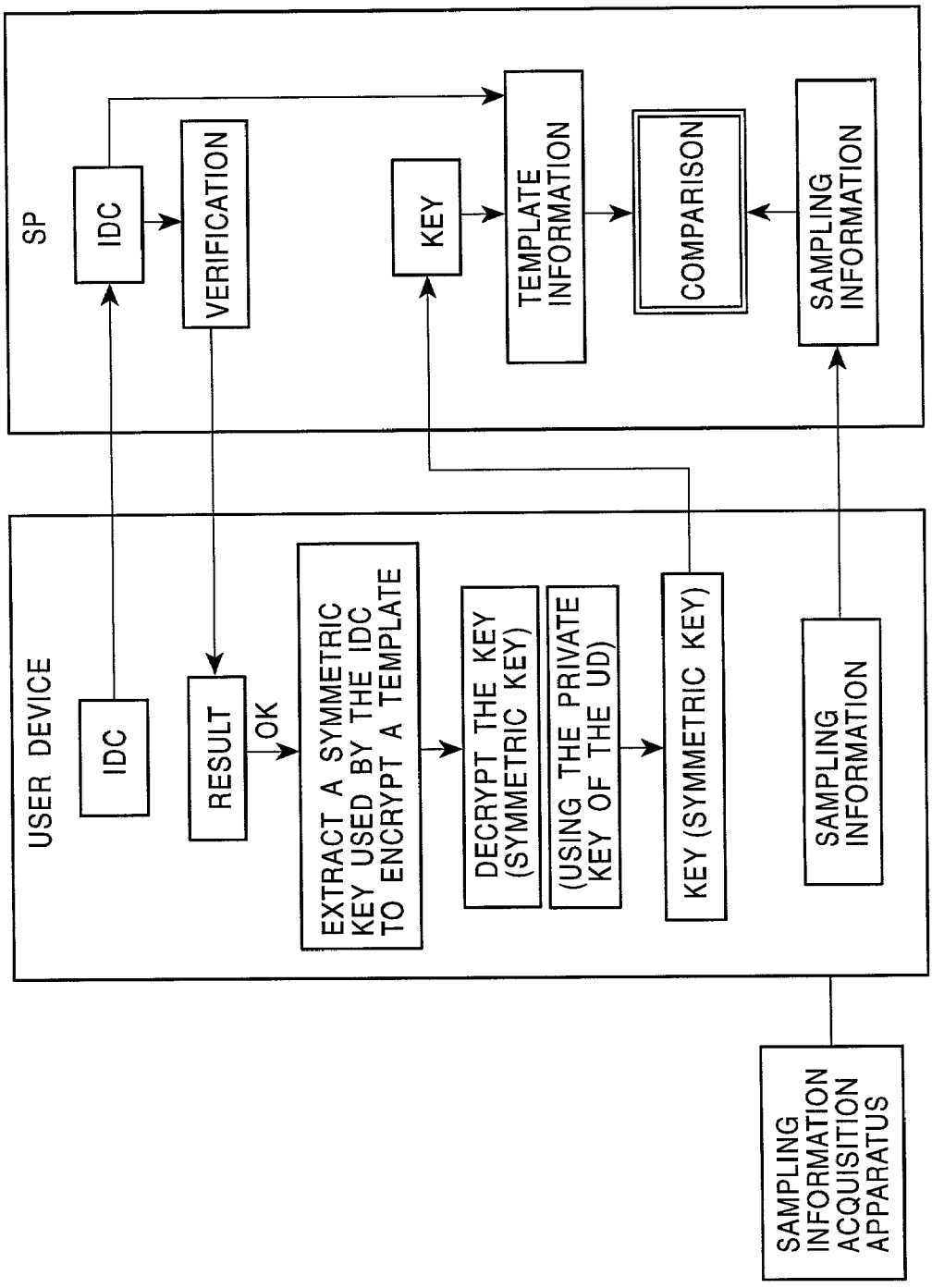

SP
IDC
VERIFICATION
KEY
TEMPLATE INFORMATION
COMPARISON
SAMPLING INFORMATION
USER DEVICE
IDC
RESULT
OK
EXTRACT A SYMMETRIC KEY USED BY THE IDC TO ENCRYPT A TEMPLATE
DECRYPT THE KEY (SYMMETRIC KEY)
(USING THE PRIVATE KEY OF THE UD)
KEY (SYMMETRIC KEY)
SAMPLING INFORMATION
SAMPLING INFORMATION ACQUISITION APPARATUS

FIG. 30

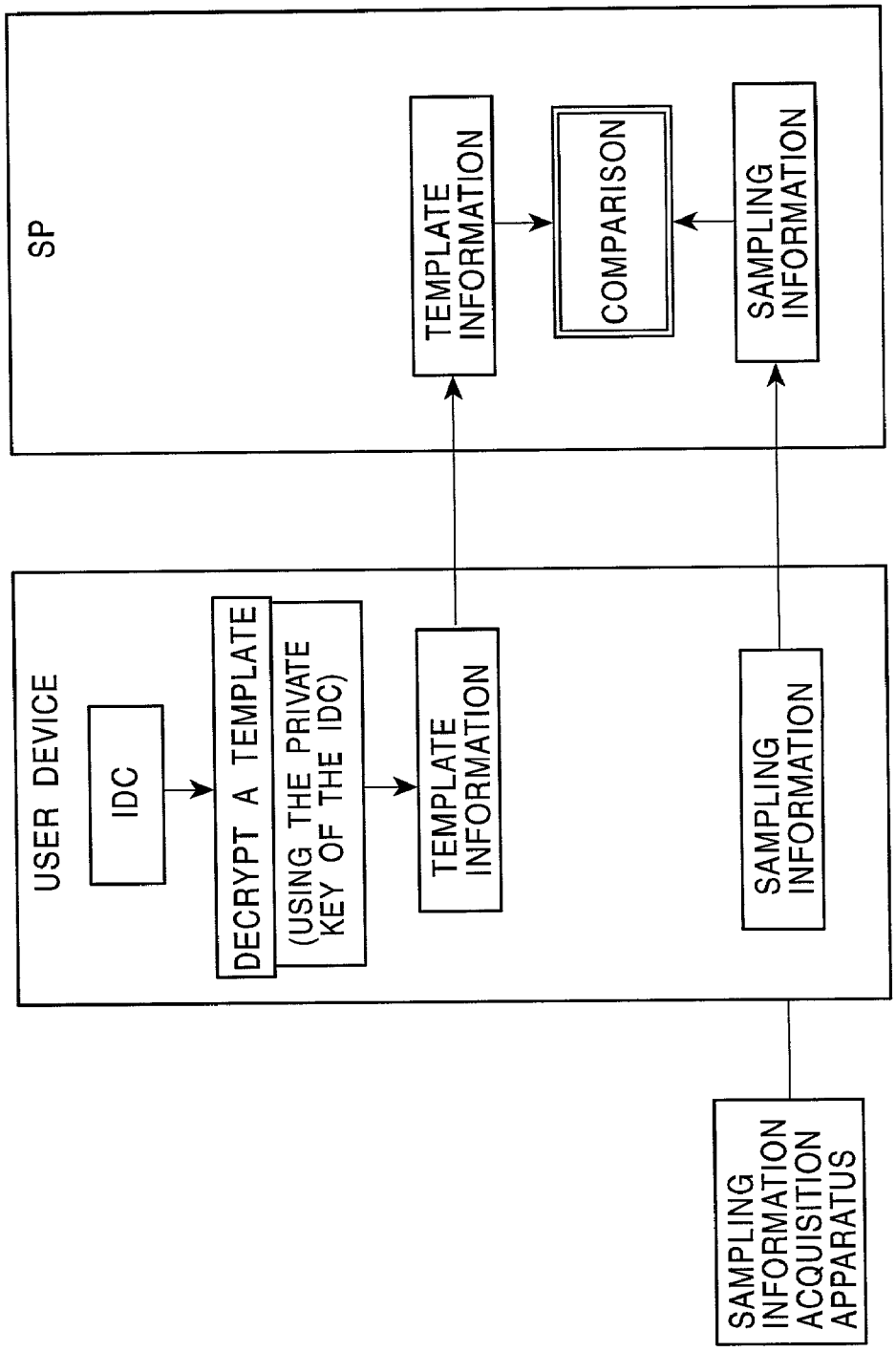

SP
TEMPLATE INFORMATION
COMPARISON
SAMPLING INFORMATION
USER DEVICE
IDC
DECRYPT A TEMPLATE
(USING THE PRIVATE KEY OF THE IDC)
TEMPLATE INFORMATION
SAMPLING INFORMATION
SAMPLING INFORMATION ACQUISITION APPARATUS

FIG. 31

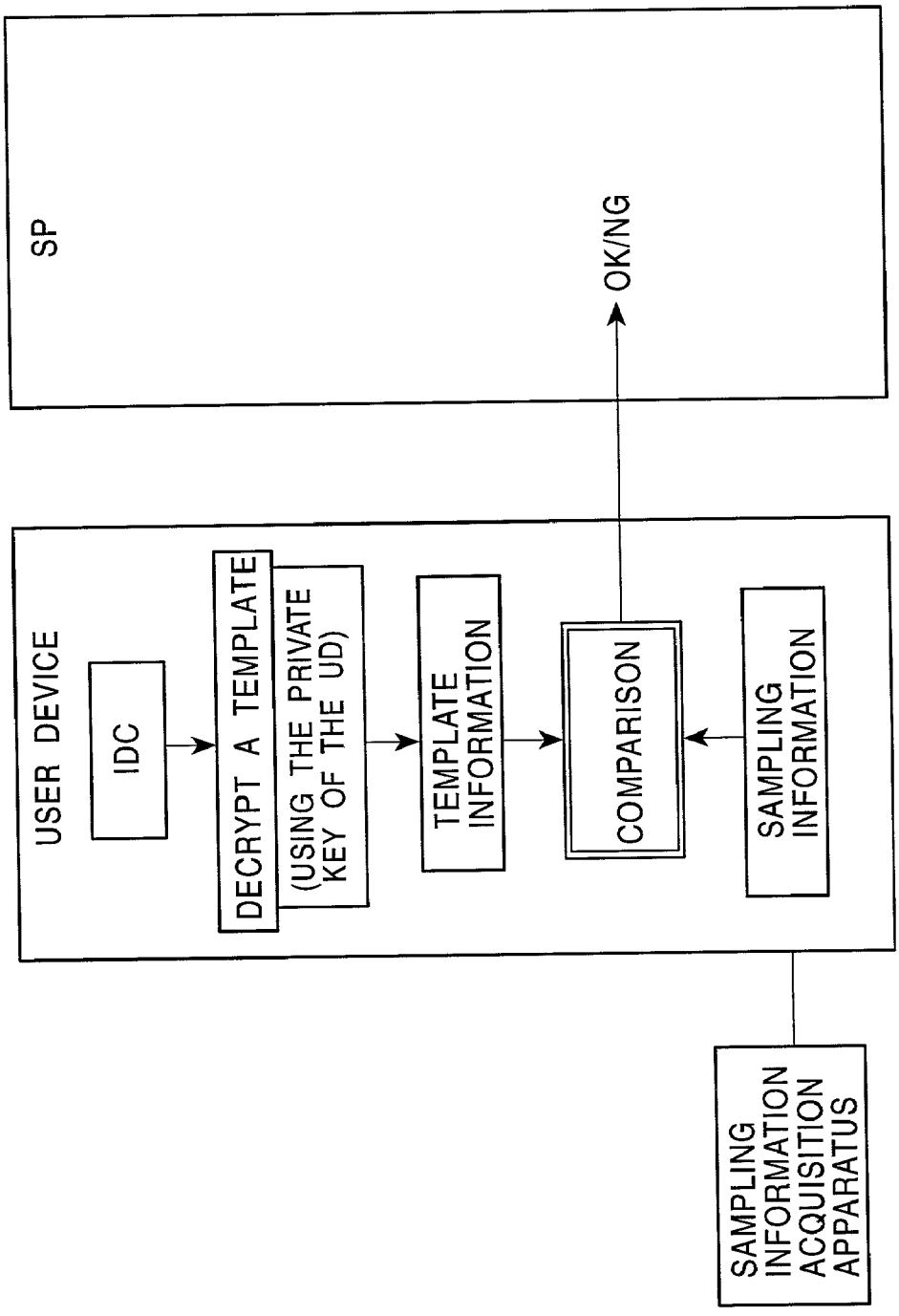

SP
OK/NG
USER DEVICE
IDC
DECRYPT A TEMPLATE
(USING THE PRIVATE KEY OF THE UD)
TEMPLATE INFORMATION
COMPARISON
SAMPLING INFORMATION
SAMPLING INFORMATION ACQUISITION APPARATUS

FIG. 32

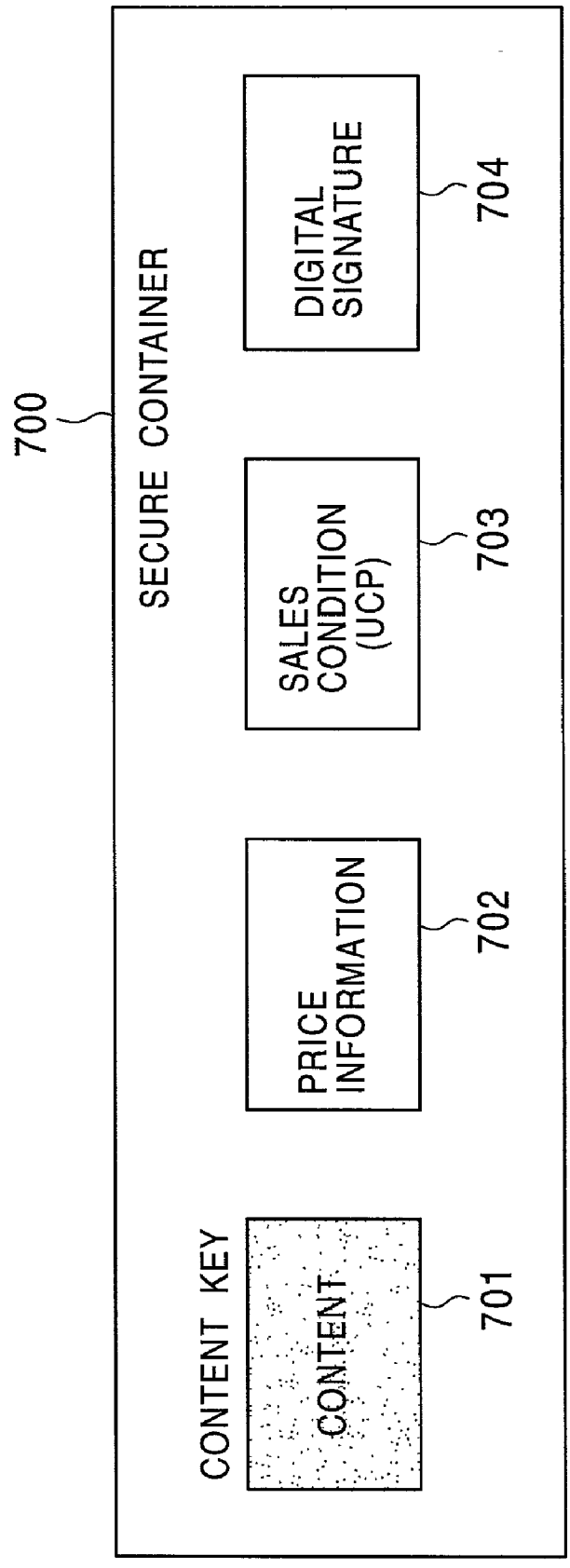

700
SECURE CONTAINER
CONTENT KEY
CONTENT
701
PRICE INFORMATION
702
SALES CONDITION (UCP)
703
DIGITAL SIGNATURE
704

FIG. 33

USER ID	IDENTIFICATION CERTIFICATE (IDC) IDENTIFIER
ABC0001	CDE00021
ABC0002	CDE00027
ABC0003	CDE03211
⋮	⋮
BBC0231	EED02333

FIG. 34

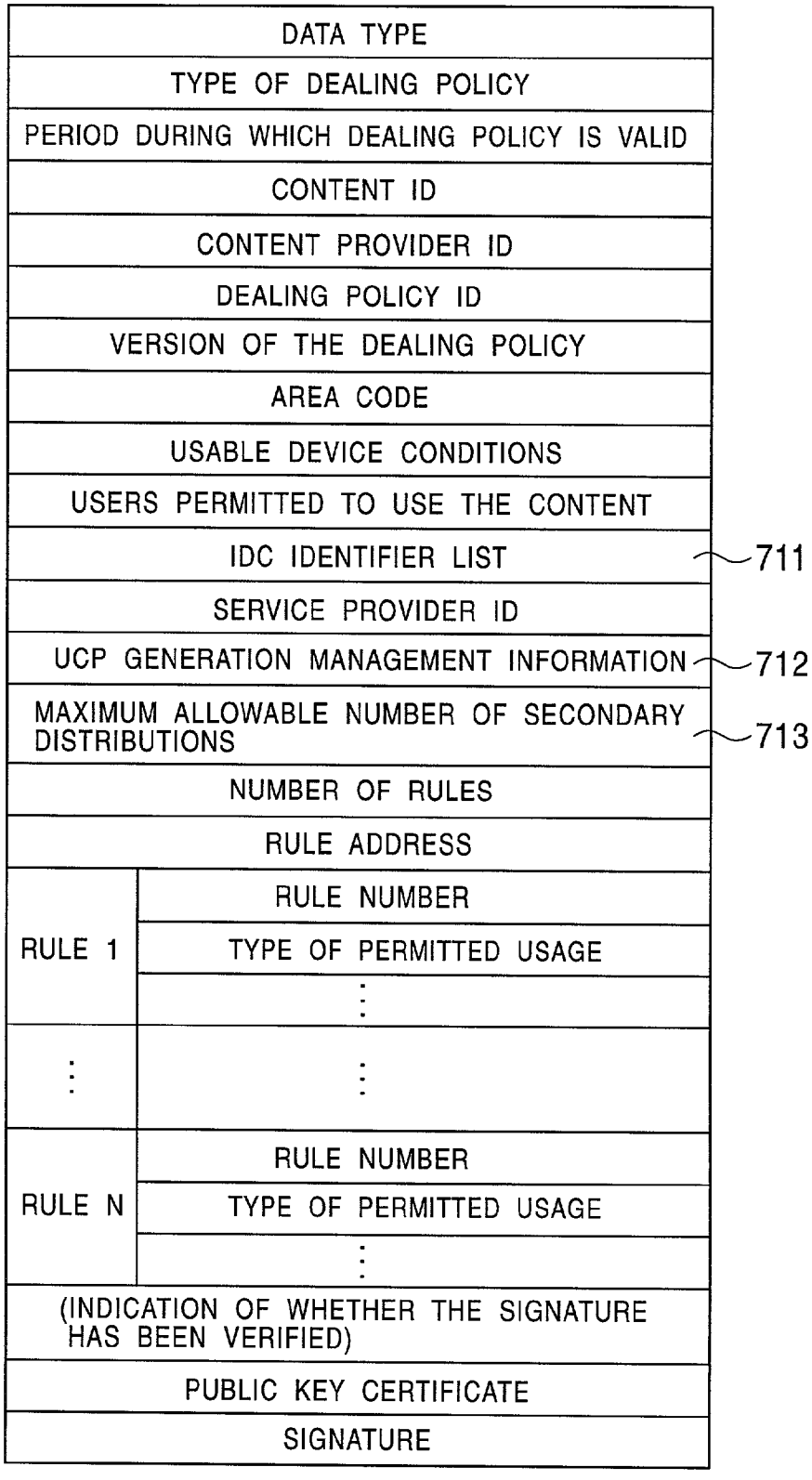

DATA TYPE
TYPE OF DEALING POLICY
PERIOD DURING WHICH DEALING POLICY IS VALID
CONTENT ID
CONTENT PROVIDER ID
DEALING POLICY ID
VERSION OF THE DEALING POLICY
AREA CODE
USABLE DEVICE CONDITIONS
USERS PERMITTED TO USE THE CONTENT
IDC IDENTIFIER LIST
711
SERVICE PROVIDER ID
UCP GENERATION MANAGEMENT INFORMATION
712
MAXIMUM ALLOWABLE NUMBER OF SECONDARY DISTRIBUTIONS
713
NUMBER OF RULES
RULE ADDRESS
RULE 1
RULE NUMBER
TYPE OF PERMITTED USAGE
RULE N
RULE NUMBER
TYPE OF PERMITTED USAGE
(INDICATION OF WHETHER THE SIGNATURE HAS BEEN VERIFIED)
PUBLIC KEY CERTIFICATE
SIGNATURE

FIG. 35

RULE NUMBER	PERMITTED USAGE	PERIOD	NUMBER OF TIMES CONTENT IS USED	COPY
1	PLAYBACK	NOT LIMITED	NOT LIMITED	—
2		LIMITED	NOT LIMITED	—
3		NOT LIMITED	LIMITED	—
4	COPY	NOT LIMITED	NOT LIMITED	NOT LIMITED
5		LIMITED	NOT LIMITED	NOT LIMITED
6		NOT LIMITED	LIMITED	NOT LIMITED
7		NOT LIMITED	NOT LIMITED	SCMS
8		LIMITED	NOT LIMITED	
9		NOT LIMITED	LIMITED	
10		NOT LIMITED	NOT LIMITED	OTHERS
11		LIMITED	NOT LIMITED	
12		NOT LIMITED	LIMITED	
13	CHANGING OF PERMITTED USAGE			
14	REDISTRIBUTION			
15	UPGRADE TO AN ALBUM			
16	PERMISSION OF TRANSFERRING MANAGEMENT			

FIG. 36

<table>
<tr><td colspan="2">DATA TYPE</td></tr>
<tr><td colspan="2">TYPE OF PRICE INFORMATION</td></tr>
<tr><td colspan="2">PERIOD DURING WHICH THE PRICE INFORMATION IS VALID</td></tr>
<tr><td colspan="2">CONTENT ID</td></tr>
<tr><td colspan="2">SERVICE PROVIDER ID</td></tr>
<tr><td colspan="2">PRICE INFORMATION ID</td></tr>
<tr><td colspan="2">VERSION OF THE PRICE INFORMATION</td></tr>
<tr><td colspan="2">AREA CODE</td></tr>
<tr><td colspan="2">USABLE DEVICE CONDITIONS</td></tr>
<tr><td colspan="2">USERS PERMITTED TO USE THE CONTENT</td></tr>
<tr><td colspan="2">IDC IDENTIFIER LIST ~721</td></tr>
<tr><td colspan="2">CONTENT PROVIDER ID</td></tr>
<tr><td colspan="2">DEALING POLICY ID</td></tr>
<tr><td colspan="2">NUMBER OF RULES</td></tr>
<tr><td colspan="2">RULE ADDRESS</td></tr>
<tr><td rowspan="3">RULE 1</td><td>RULE NUMBER</td></tr>
<tr><td>⋮</td></tr>
<tr><td>⋮</td></tr>
<tr><td>⋮</td><td>⋮</td></tr>
<tr><td rowspan="3">RULE N</td><td>RULE NUMBER</td></tr>
<tr><td>⋮</td></tr>
<tr><td>⋮</td></tr>
<tr><td colspan="2">(INDICATION OF WHETHER THE SIGNATURE HAS BEEN VERIFIED)</td></tr>
<tr><td colspan="2">PUBLIC KEY CERTIFICATE</td></tr>
<tr><td colspan="2">SIGNATURE</td></tr>
</table>

FIG. 37

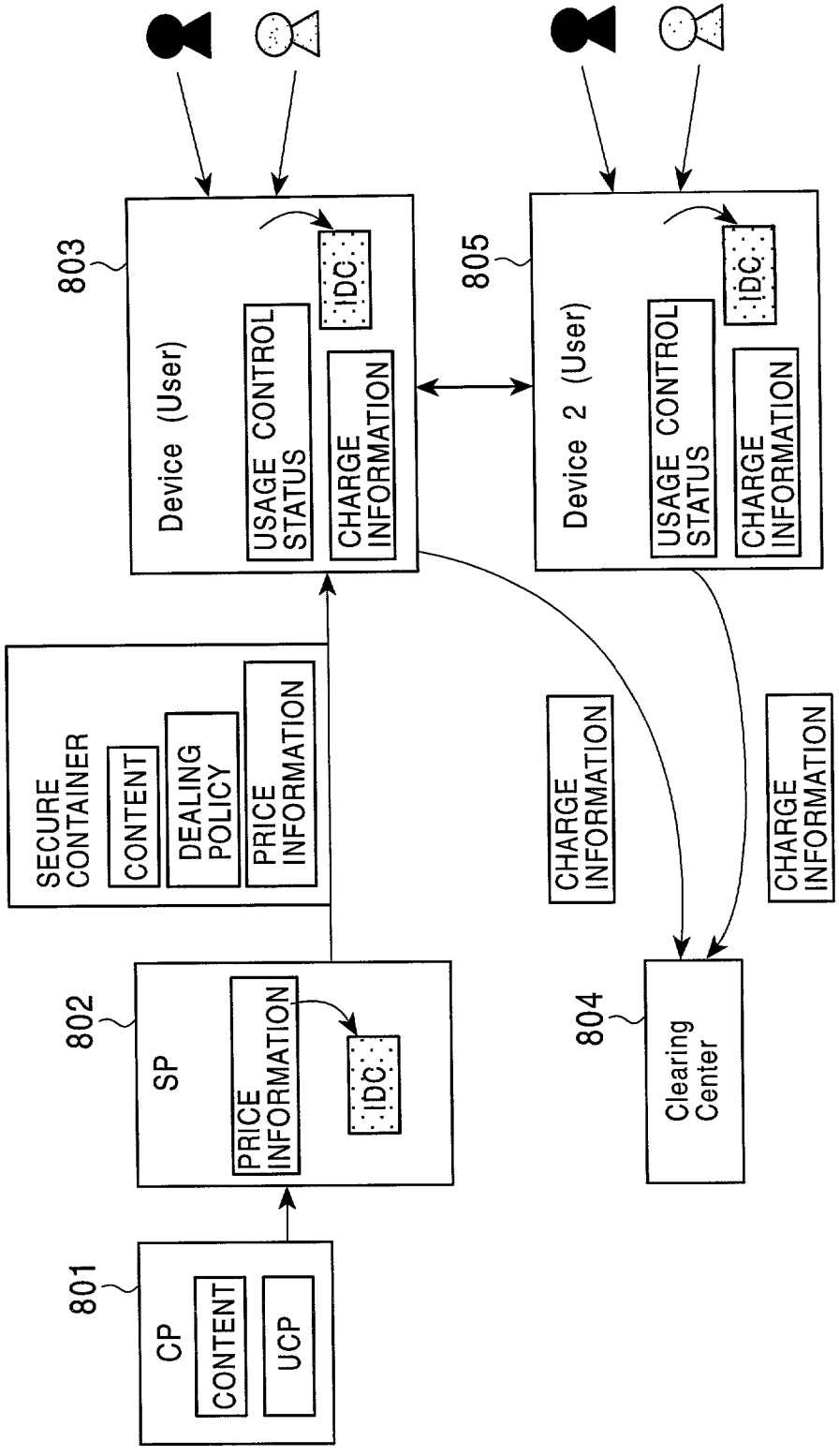

803
Device (User)
USAGE CONTROL STATUS
CHARGE INFORMATION
IDC
805
Device 2 (User)
USAGE CONTROL STATUS
CHARGE INFORMATION
IDC
SECURE CONTAINER
CONTENT
DEALING POLICY
PRICE INFORMATION
CHARGE INFORMATION
CHARGE INFORMATION
802
SP
PRICE INFORMATION
IDC
804
Clearing Center
801
CP
CONTENT
UCP

FIG. 38

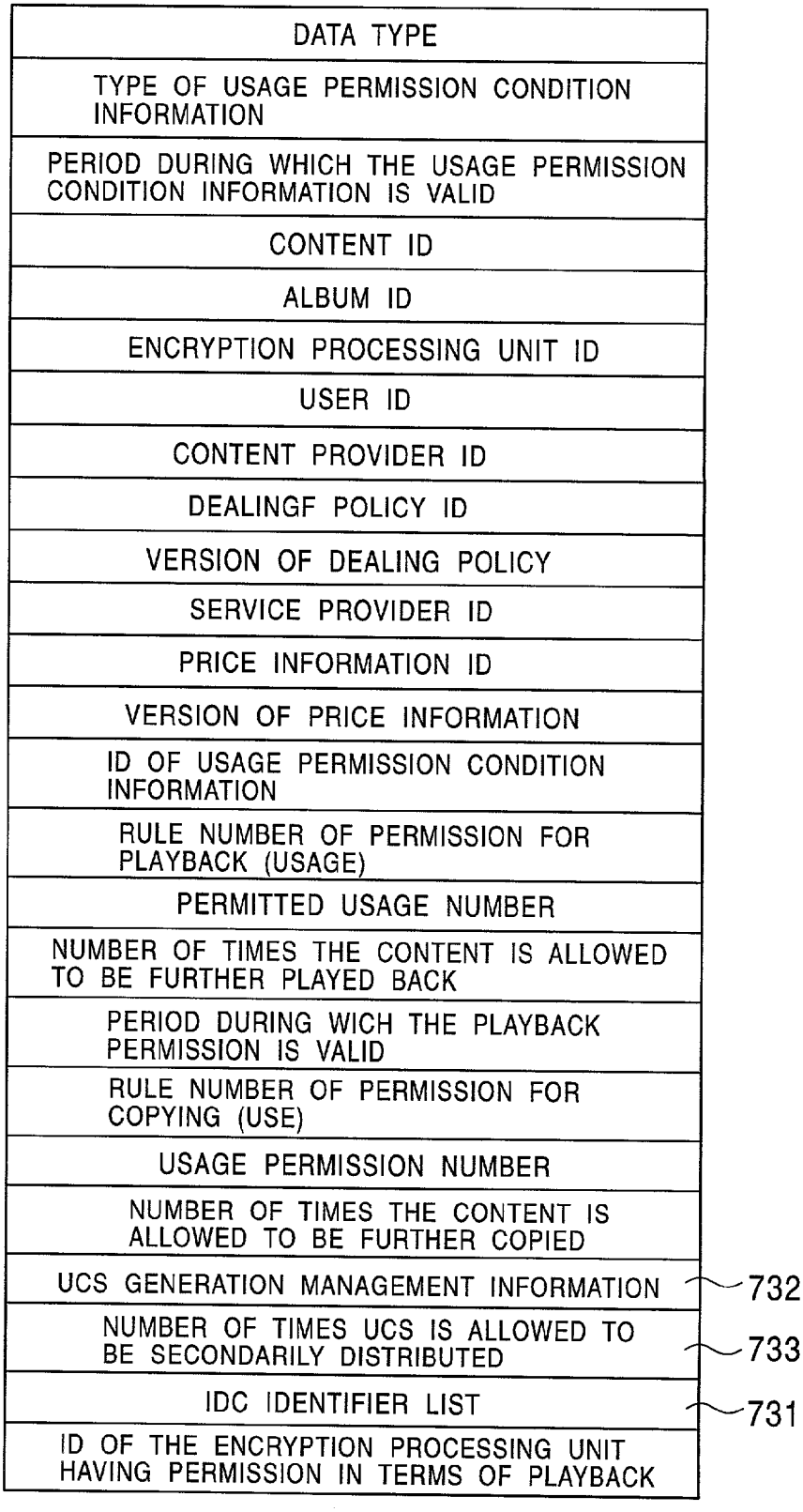

DATA TYPE
TYPE OF USAGE PERMISSION CONDITION INFORMATION
PERIOD DURING WHICH THE USAGE PERMISSION CONDITION INFORMATION IS VALID
CONTENT ID
ALBUM ID
ENCRYPTION PROCESSING UNIT ID
USER ID
CONTENT PROVIDER ID
DEALINGF POLICY ID
VERSION OF DEALING POLICY
SERVICE PROVIDER ID
PRICE INFORMATION ID
VERSION OF PRICE INFORMATION
ID OF USAGE PERMISSION CONDITION INFORMATION
RULE NUMBER OF PERMISSION FOR PLAYBACK (USAGE)
PERMITTED USAGE NUMBER
NUMBER OF TIMES THE CONTENT IS ALLOWED TO BE FURTHER PLAYED BACK
PERIOD DURING WICH THE PLAYBACK PERMISSION IS VALID
RULE NUMBER OF PERMISSION FOR COPYING (USE)
USAGE PERMISSION NUMBER
NUMBER OF TIMES THE CONTENT IS ALLOWED TO BE FURTHER COPIED
UCS GENERATION MANAGEMENT INFORMATION
732
NUMBER OF TIMES UCS IS ALLOWED TO BE SECONDARILY DISTRIBUTED
733
IDC IDENTIFIER LIST
731
ID OF THE ENCRYPTION PROCESSING UNIT HAVING PERMISSION IN TERMS OF PLAYBACK

FIG. 39

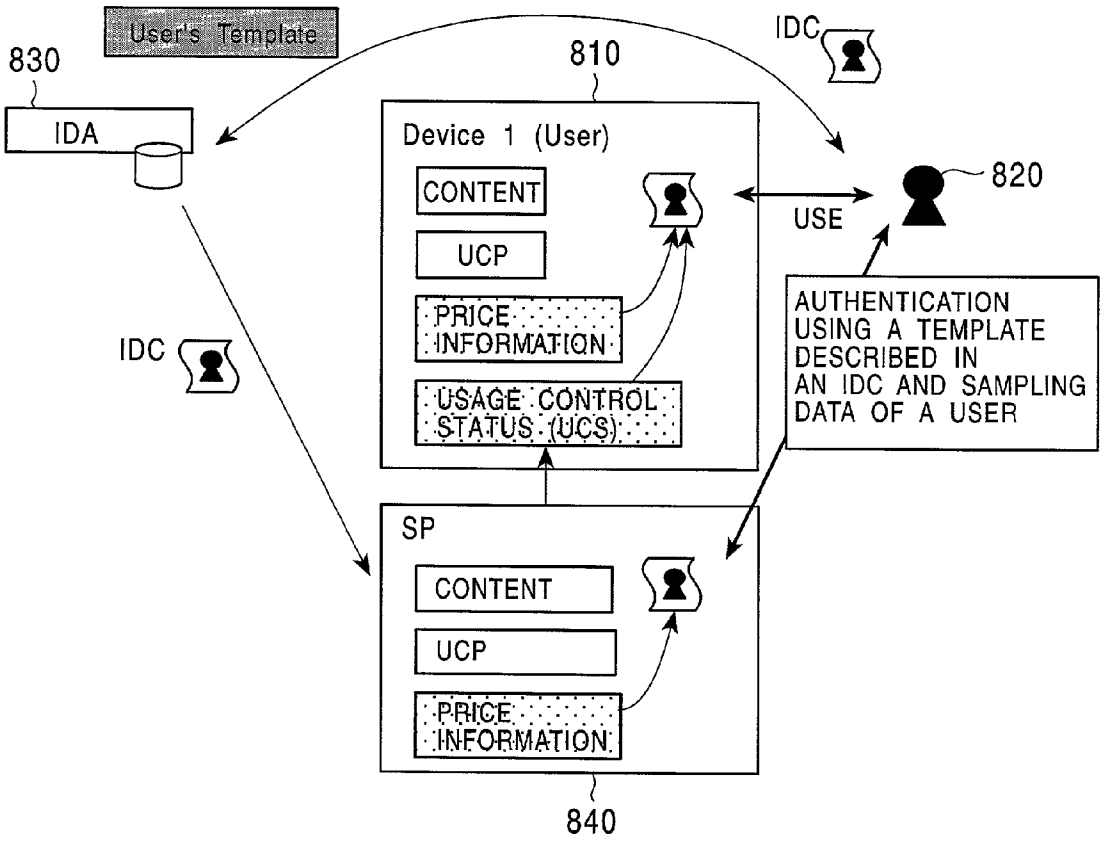

User's Template
830
IDA
IDC
810
Device 1 (User)
CONTENT
UCP
PRICE INFORMATION
USAGE CONTROL STATUS (UCS)
IDC
820
USE
AUTHENTICATION USING A TEMPLATE DESCRIBED IN AN IDC AND SAMPLING DATA OF A USER
SP
CONTENT
UCP
PRICE INFORMATION
840

FIG. 40

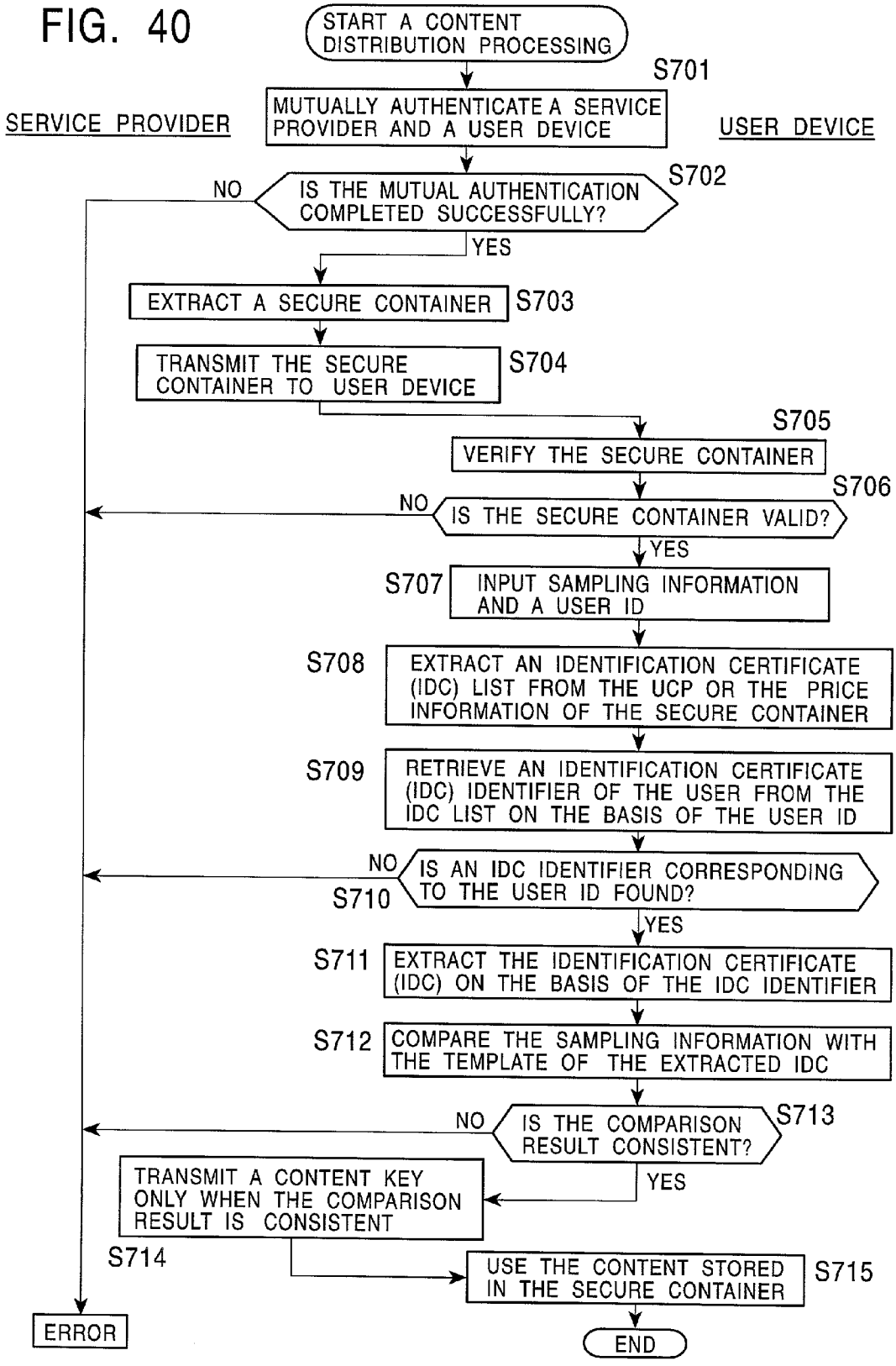

START A CONTENT DISTRIBUTION PROCESSING
S701
SERVICE PROVIDER
MUTUALLY AUTHENTICATE A SERVICE PROVIDER AND A USER DEVICE
USER DEVICE
NO
IS THE MUTUAL AUTHENTICATION COMPLETED SUCCESSFULLY?
S702
YES
EXTRACT A SECURE CONTAINER
S703
TRANSMIT THE SECURE CONTAINER TO USER DEVICE
S704
S705
VERIFY THE SECURE CONTAINER
S706
NO
IS THE SECURE CONTAINER VALID?
YES
S707
INPUT SAMPLING INFORMATION AND A USER ID
S708
EXTRACT AN IDENTIFICATION CERTIFICATE (IDC) LIST FROM THE UCP OR THE PRICE INFORMATION OF THE SECURE CONTAINER
S709
RETRIEVE AN IDENTIFICATION CERTIFICATE (IDC) IDENTIFIER OF THE USER FROM THE IDC LIST ON THE BASIS OF THE USER ID
NO
S710
IS AN IDC IDENTIFIER CORRESPONDING TO THE USER ID FOUND?
YES
S711
EXTRACT THE IDENTIFICATION CERTIFICATE (IDC) ON THE BASIS OF THE IDC IDENTIFIER
S712
COMPARE THE SAMPLING INFORMATION WITH THE TEMPLATE OF THE EXTRACTED IDC
NO
IS THE COMPARISON RESULT CONSISTENT?
S713
YES
TRANSMIT A CONTENT KEY ONLY WHEN THE COMPARISON RESULT IS CONSISTENT
S714
USE THE CONTENT STORED IN THE SECURE CONTAINER
S715
ERROR
END

FIG. 41

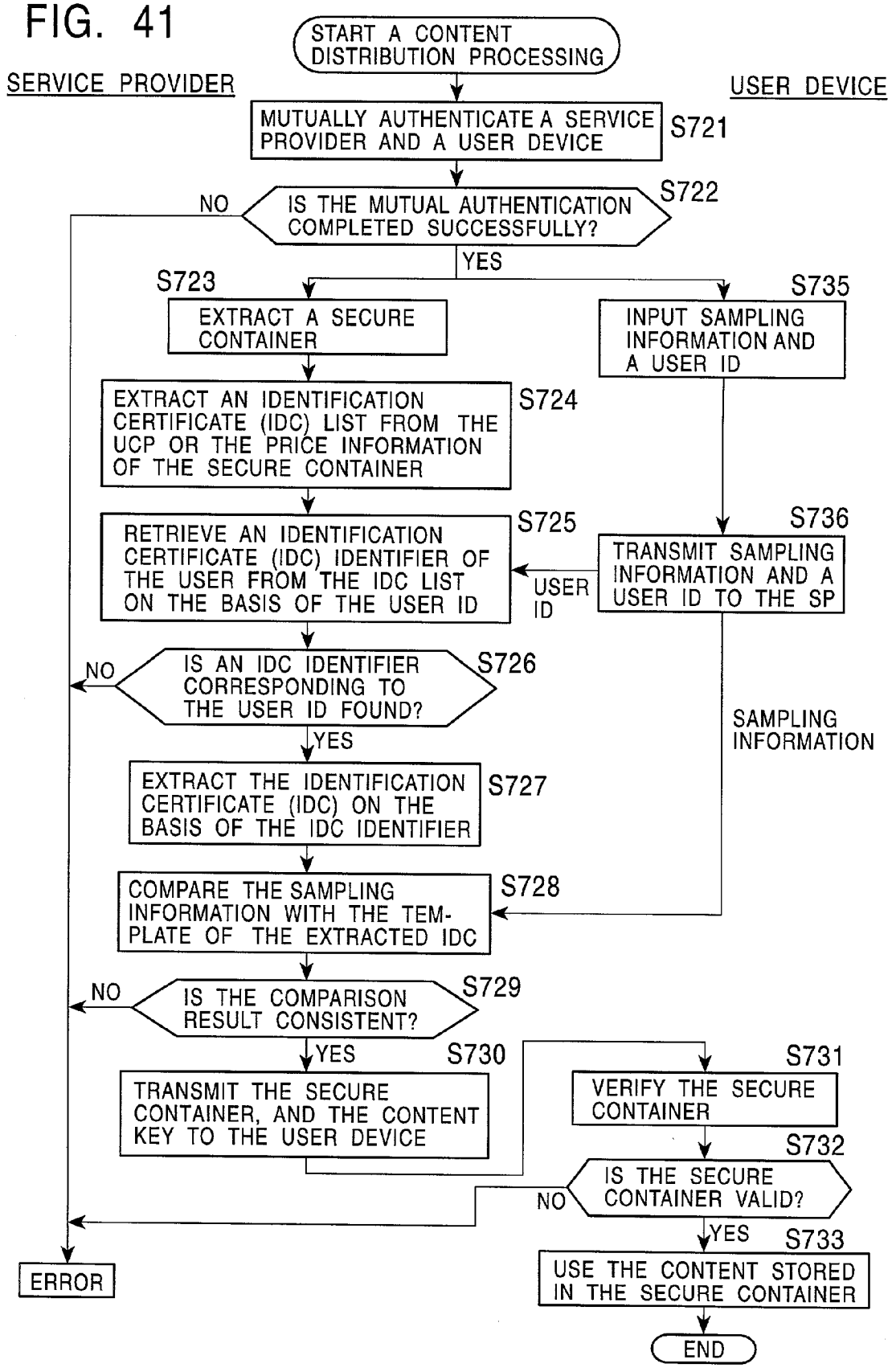

SERVICE PROVIDER
USER DEVICE
START A CONTENT DISTRIBUTION PROCESSING
MUTUALLY AUTHENTICATE A SERVICE PROVIDER AND A USER DEVICE
S721
IS THE MUTUAL AUTHENTICATION COMPLETED SUCCESSFULLY?
S722
NO
YES
S723
EXTRACT A SECURE CONTAINER
S735
INPUT SAMPLING INFORMATION AND A USER ID
EXTRACT AN IDENTIFICATION CERTIFICATE (IDC) LIST FROM THE UCP OR THE PRICE INFORMATION OF THE SECURE CONTAINER
S724
RETRIEVE AN IDENTIFICATION CERTIFICATE (IDC) IDENTIFIER OF THE USER FROM THE IDC LIST ON THE BASIS OF THE USER ID
S725
S736
TRANSMIT SAMPLING INFORMATION AND A USER ID TO THE SP
USER ID
IS AN IDC IDENTIFIER CORRESPONDING TO THE USER ID FOUND?
S726
NO
YES
SAMPLING INFORMATION
EXTRACT THE IDENTIFICATION CERTIFICATE (IDC) ON THE BASIS OF THE IDC IDENTIFIER
S727
COMPARE THE SAMPLING INFORMATION WITH THE TEMPLATE OF THE EXTRACTED IDC
S728
IS THE COMPARISON RESULT CONSISTENT?
S729
NO
YES
S730
TRANSMIT THE SECURE CONTAINER, AND THE CONTENT KEY TO THE USER DEVICE
S731
VERIFY THE SECURE CONTAINER
S732
IS THE SECURE CONTAINER VALID?
NO
YES
S733
USE THE CONTENT STORED IN THE SECURE CONTAINER
ERROR
END

FIG. 42

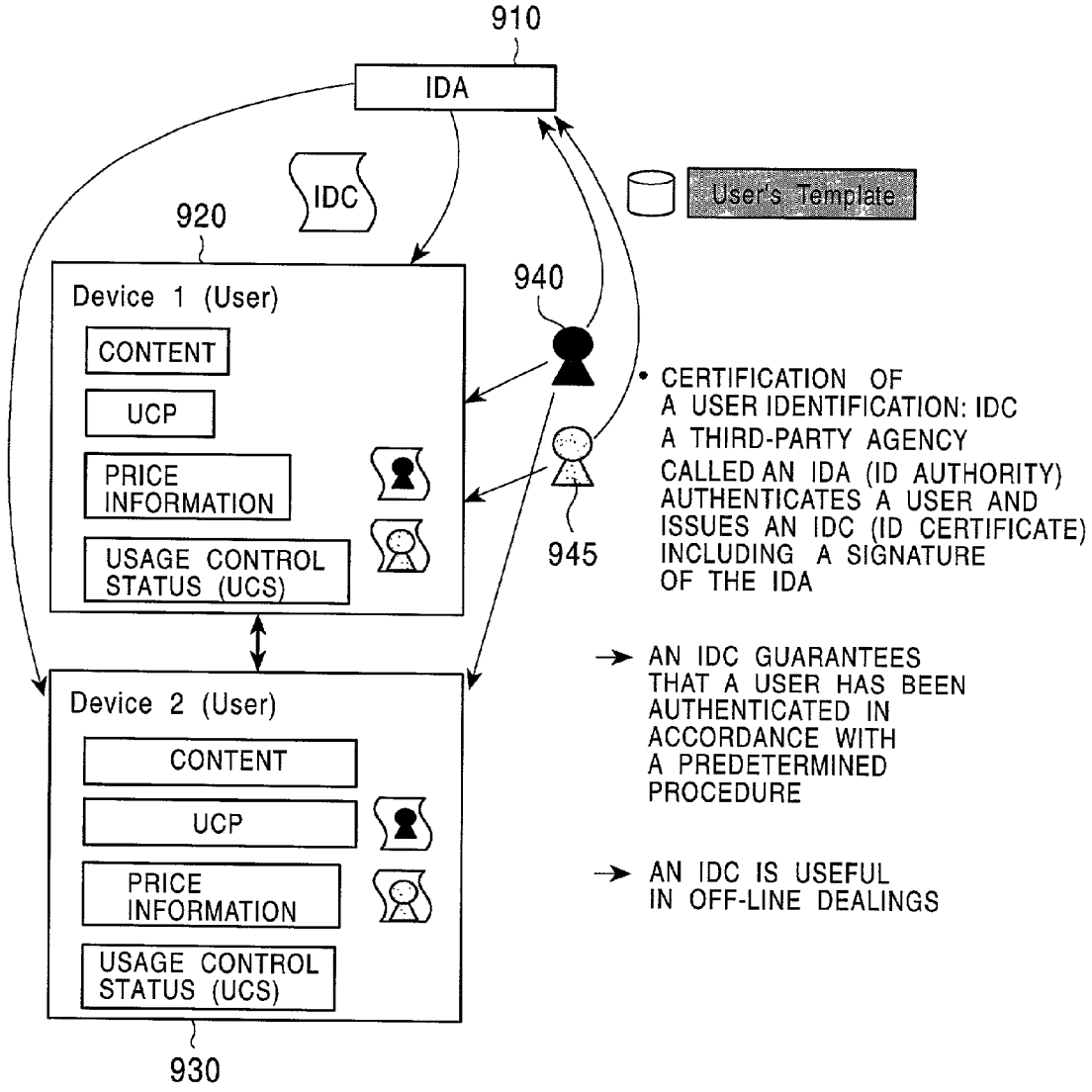

910
IDA
IDC
User's Template
920
940
Device 1 (User)
CONTENT
UCP
PRICE INFORMATION
USAGE CONTROL STATUS (UCS)
945
• CERTIFICATION OF A USER IDENTIFICATION: IDC A THIRD-PARTY AGENCY CALLED AN IDA (ID AUTHORITY) AUTHENTICATES A USER AND ISSUES AN IDC (ID CERTIFICATE) INCLUDING A SIGNATURE OF THE IDA
→ AN IDC GUARANTEES THAT A USER HAS BEEN AUTHENTICATED IN ACCORDANCE WITH A PREDETERMINED PROCEDURE
→ AN IDC IS USEFUL IN OFF-LINE DEALINGS
Device 2 (User)
CONTENT
UCP
PRICE INFORMATION
USAGE CONTROL STATUS (UCS)
930

FIG. 43

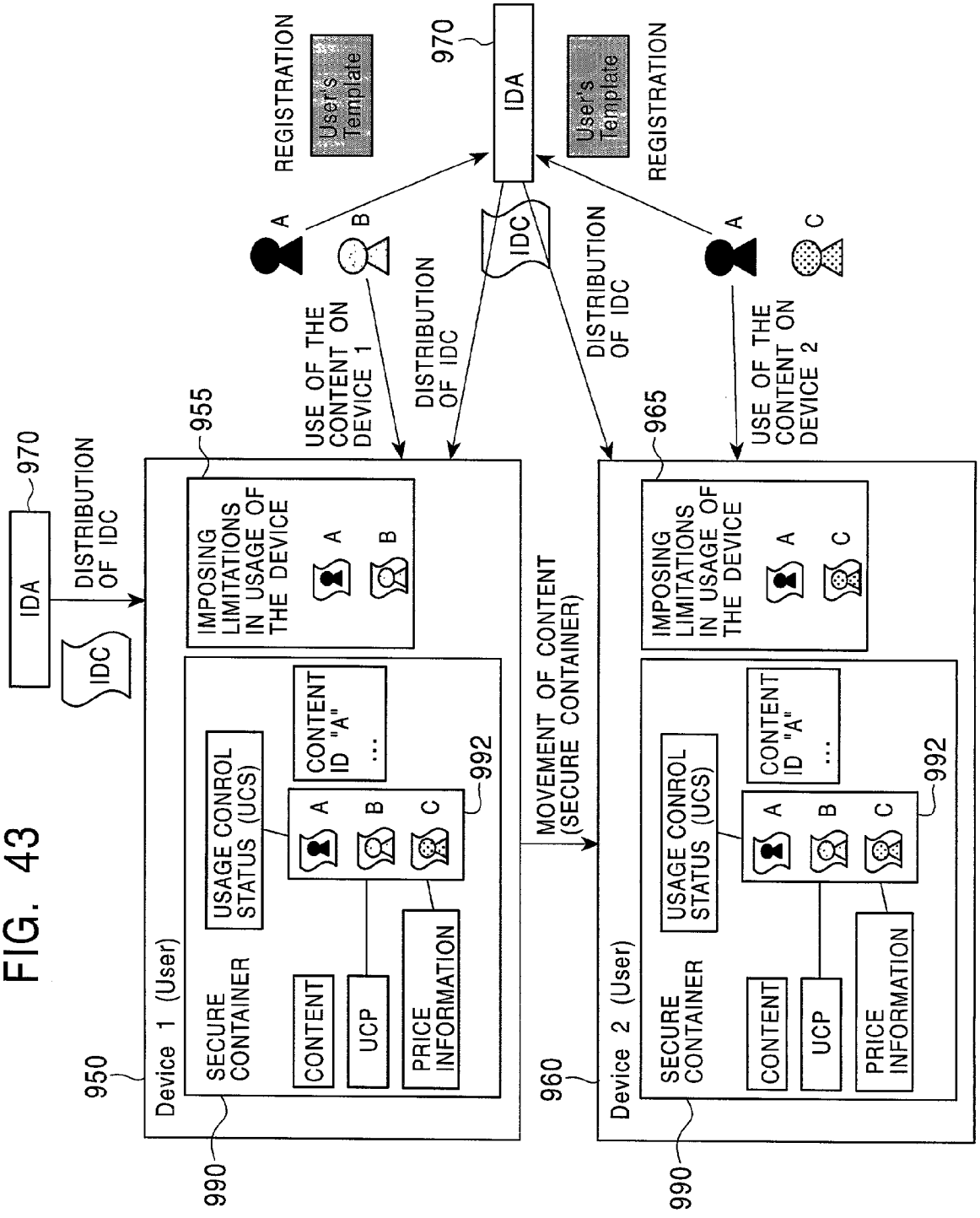

970
IDA
DISTRIBUTION OF IDC
IDC
950
Device 1 (User)
990
955
IMPOSING LIMITATIONS IN USAGE OF THE DEVICE
A
B
USAGE CONROL STATUS (UCS)
CONTENT ID "A"
...
992
SECURE CONTAINER
CONTENT
UCP
PRICE INFORMATION
USE OF THE CONTENT ON DEVICE 1
DISTRIBUTION OF IDC
REGISTRATION
User's Template
970
IDA
IDC
DISTRIBUTION OF IDC
REGISTRATION
User's Template
MOVEMENT OF CONTENT (SECURE CONTAINER)
960
Device 2 (User)
990
965
IMPOSING LIMITATIONS IN USAGE OF THE DEVICE
A
C
USAGE CONROL STATUS (UCS)
CONTENT ID "A"
...
992
SECURE CONTAINER
CONTENT
UCP
PRICE INFORMATION
USE OF THE CONTENT ON DEVICE 2

FIG. 44

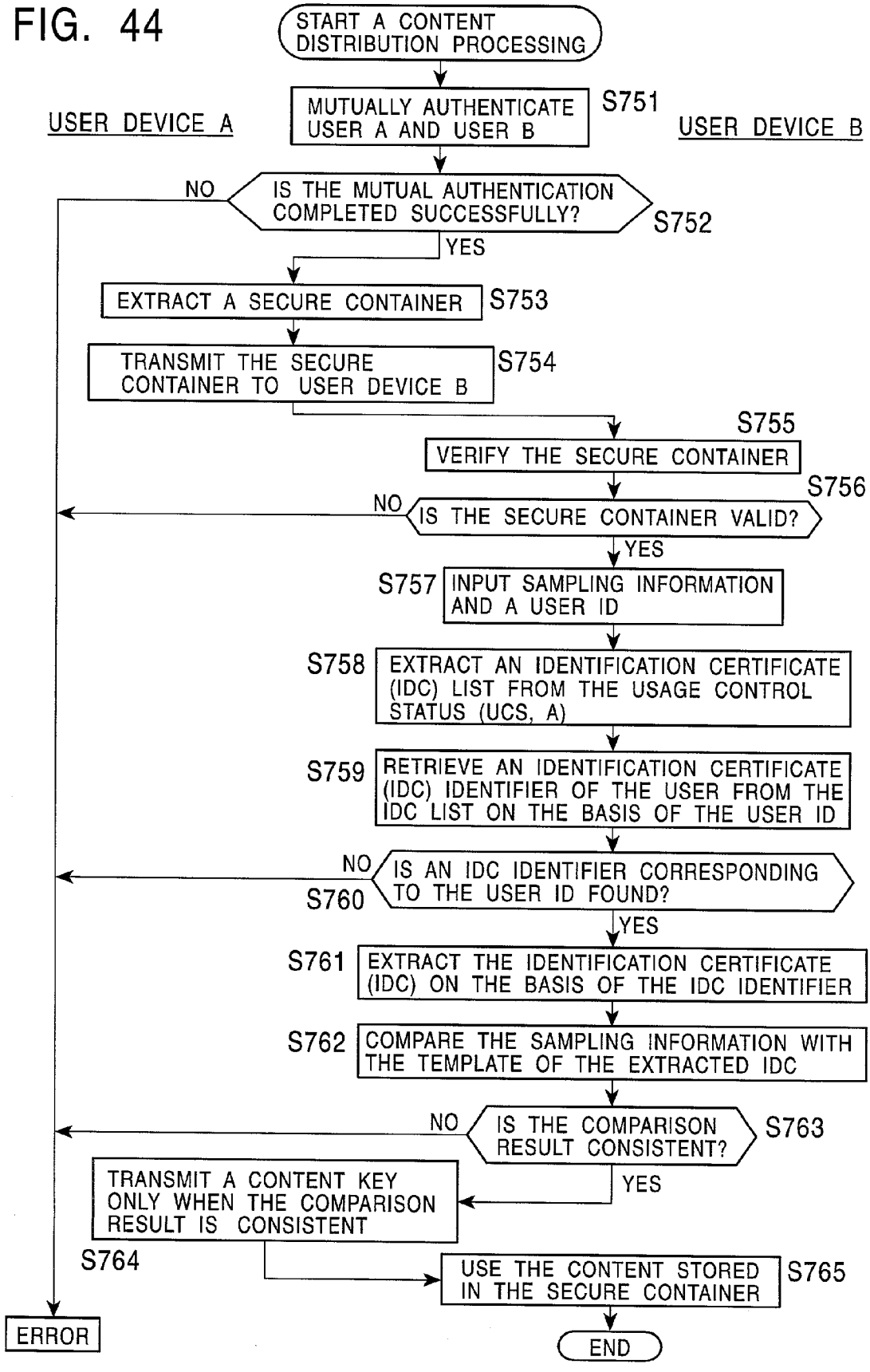

START A CONTENT DISTRIBUTION PROCESSING
USER DEVICE A
MUTUALLY AUTHENTICATE USER A AND USER B
S751
USER DEVICE B
NO
IS THE MUTUAL AUTHENTICATION COMPLETED SUCCESSFULLY?
S752
YES
EXTRACT A SECURE CONTAINER
S753
TRANSMIT THE SECURE CONTAINER TO USER DEVICE B
S754
S755
VERIFY THE SECURE CONTAINER
S756
NO
IS THE SECURE CONTAINER VALID?
YES
S757
INPUT SAMPLING INFORMATION AND A USER ID
S758
EXTRACT AN IDENTIFICATION CERTIFICATE (IDC) LIST FROM THE USAGE CONTROL STATUS (UCS, A)
S759
RETRIEVE AN IDENTIFICATION CERTIFICATE (IDC) IDENTIFIER OF THE USER FROM THE IDC LIST ON THE BASIS OF THE USER ID
NO
S760
IS AN IDC IDENTIFIER CORRESPONDING TO THE USER ID FOUND?
YES
S761
EXTRACT THE IDENTIFICATION CERTIFICATE (IDC) ON THE BASIS OF THE IDC IDENTIFIER
S762
COMPARE THE SAMPLING INFORMATION WITH THE TEMPLATE OF THE EXTRACTED IDC
NO
IS THE COMPARISON RESULT CONSISTENT?
S763
YES
TRANSMIT A CONTENT KEY ONLY WHEN THE COMPARISON RESULT IS CONSISTENT
S764
USE THE CONTENT STORED IN THE SECURE CONTAINER
S765
ERROR
END

FIG. 45

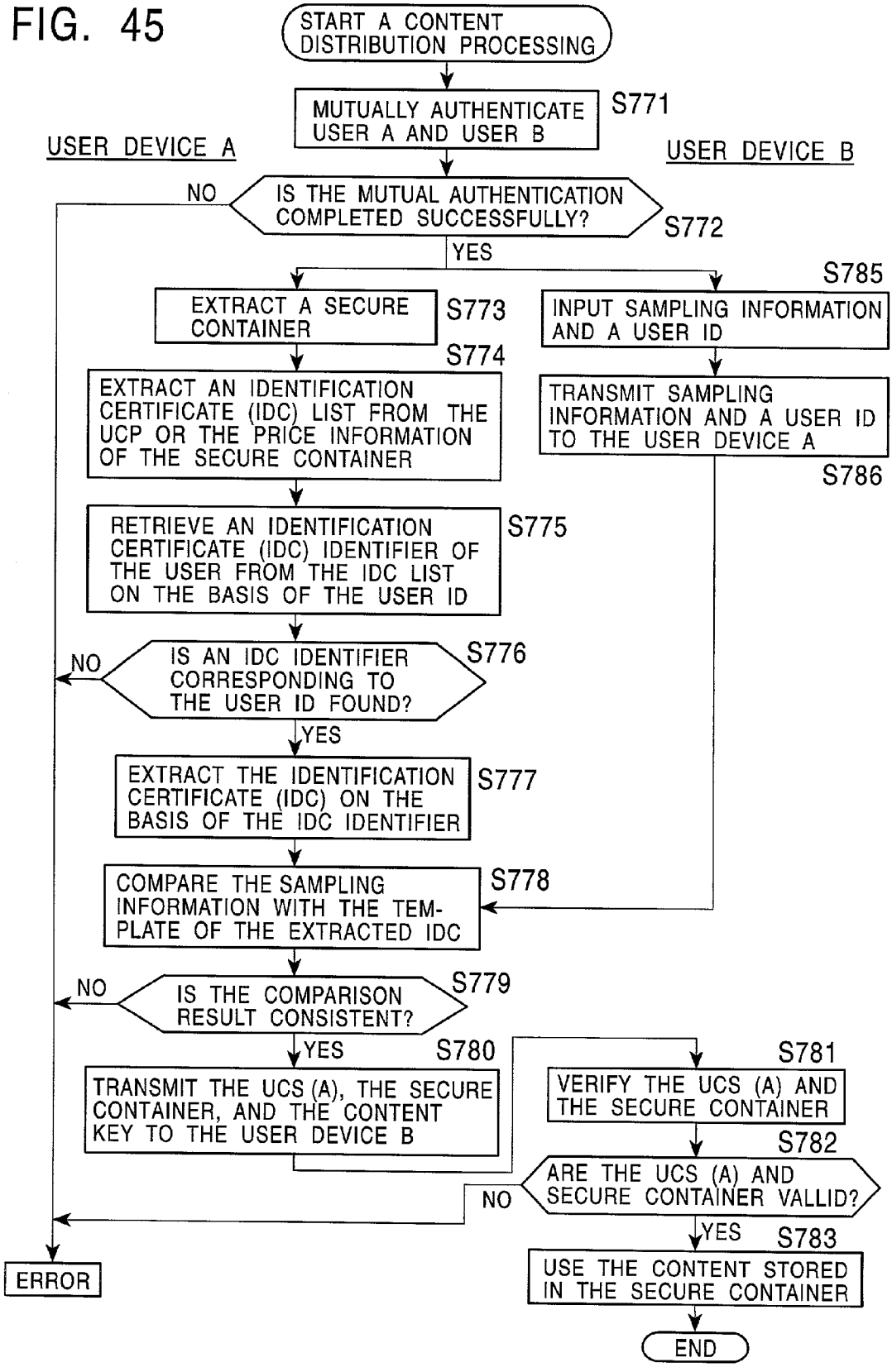

START A CONTENT DISTRIBUTION PROCESSING
MUTUALLY AUTHENTICATE USER A AND USER B
S771
USER DEVICE A
USER DEVICE B
NO
IS THE MUTUAL AUTHENTICATION COMPLETED SUCCESSFULLY?
S772
YES
S785
EXTRACT A SECURE CONTAINER
S773
INPUT SAMPLING INFORMATION AND A USER ID
S774
EXTRACT AN IDENTIFICATION CERTIFICATE (IDC) LIST FROM THE UCP OR THE PRICE INFORMATION OF THE SECURE CONTAINER
TRANSMIT SAMPLING INFORMATION AND A USER ID TO THE USER DEVICE A
S786
RETRIEVE AN IDENTIFICATION CERTIFICATE (IDC) IDENTIFIER OF THE USER FROM THE IDC LIST ON THE BASIS OF THE USER ID
S775
NO
IS AN IDC IDENTIFIER CORRESPONDING TO THE USER ID FOUND?
S776
YES
EXTRACT THE IDENTIFICATION CERTIFICATE (IDC) ON THE BASIS OF THE IDC IDENTIFIER
S777
COMPARE THE SAMPLING INFORMATION WITH THE TEMPLATE OF THE EXTRACTED IDC
S778
NO
IS THE COMPARISON RESULT CONSISTENT?
S779
YES
S780
TRANSMIT THE UCS (A), THE SECURE CONTAINER, AND THE CONTENT KEY TO THE USER DEVICE B
S781
VERIFY THE UCS (A) AND THE SECURE CONTAINER
S782
ARE THE UCS (A) AND SECURE CONTAINER VALLID?
NO
YES
S783
USE THE CONTENT STORED IN THE SECURE CONTAINER
ERROR
END

FIG. 46

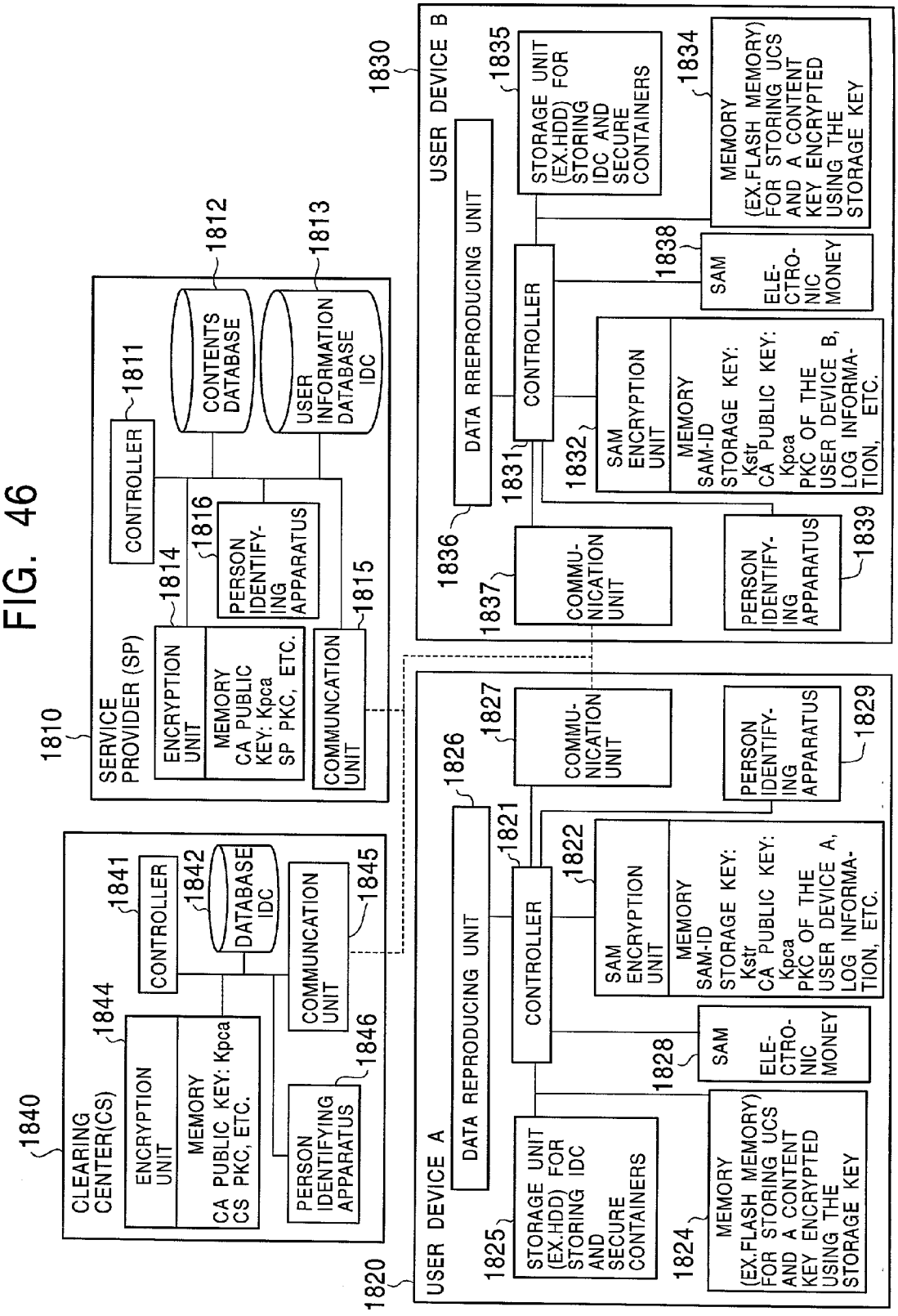

1840
CLEARING CENTER(CS)
ENCRYPTION UNIT
MEMORY
CA PUBLIC KEY: Kpca
CS PKC, ETC.
1844
PERSON IDENTIFYING APPARATUS
1846
CONTROLLER
1841
DATABASE IDC
1842
COMMUNCATION UNIT
1845
1810
SERVICE PROVIDER (SP)
ENCRYPTION UNIT
MEMORY
CA PUBLIC KEY: Kpca
SP PKC, ETC.
1814
CONTROLLER
1811
PERSON IDENTIFY-ING APPARATUS
1816
COMMUNCATION UNIT
1815
CONTENTS DATABASE
1812
USER INFORMATION DATABASE IDC
1813
1820
USER DEVICE A
DATA REPRODUCING UNIT
1826
CONTROLLER
1821
COMMU-NICATION UNIT
1827
PERSON IDENTIFY-ING APPARATUS
1829
STORAGE UNIT (EX.HDD) FOR STORING IDC AND SECURE CONTAINERS
1825
SAM ENCRYPTION UNIT
MEMORY
SAM-ID
STORAGE KEY: Kstr
CA PUBLIC KEY: Kpca
PKC OF THE USER DEVICE A, LOG INFORMA-TION, ETC.
1822
MEMORY (EX.FLASH MEMORY) FOR STORING UCS AND A CONTENT KEY ENCRYPTED USING THE STORAGE KEY
1824
SAM
ELE-CTRO-NIC MONEY
1828
1830
USER DEVICE B
DATA RREPRODUCING UNIT
1836
CONTROLLER
1831
COMMU-NICATION UNIT
1837
STORAGE UNIT (EX.HDD) FOR STORING IDC AND SECURE CONTAINERS
1835
SAM ENCRYPTION UNIT
MEMORY
SAM-ID
STORAGE KEY: Kstr
CA PUBLIC KEY: Kpca
PKC OF THE USER DEVICE B, LOG INFORMA-TION, ETC.
1832
MEMORY (EX.FLASH MEMORY) FOR STORING UCS AND A CONTENT KEY ENCRYPTED USING THE STORAGE KEY
1834
SAM
ELE-CTRO-NIC MONEY
1838
PERSON IDENTIFY-ING APPARATUS
1839

FIG. 47A

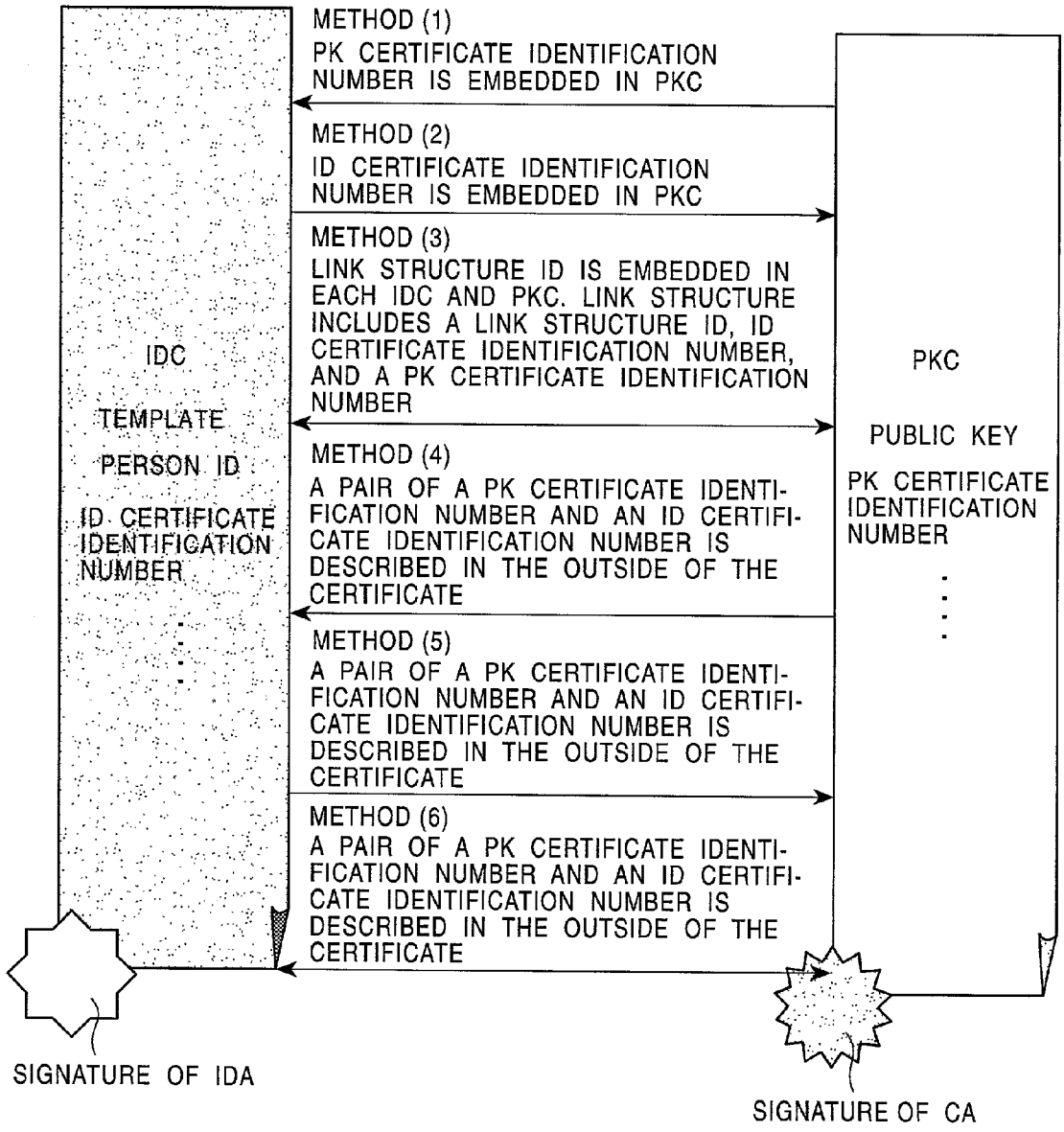

METHOD (1)
PK CERTIFICATE IDENTIFICATION NUMBER IS EMBEDDED IN PKC
METHOD (2)
ID CERTIFICATE IDENTIFICATION NUMBER IS EMBEDDED IN PKC
METHOD (3)
LINK STRUCTURE ID IS EMBEDDED IN EACH IDC AND PKC. LINK STRUCTURE INCLUDES A LINK STRUCTURE ID, ID CERTIFICATE IDENTIFICATION NUMBER, AND A PK CERTIFICATE IDENTIFICATION NUMBER
METHOD (4)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (5)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (6)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
IDC
TEMPLATE
PERSON ID
ID CERTIFICATE IDENTIFICATION NUMBER
PKC
PUBLIC KEY
PK CERTIFICATE IDENTIFICATION NUMBER
SIGNATURE OF IDA
SIGNATURE OF CA

FIG. 47B

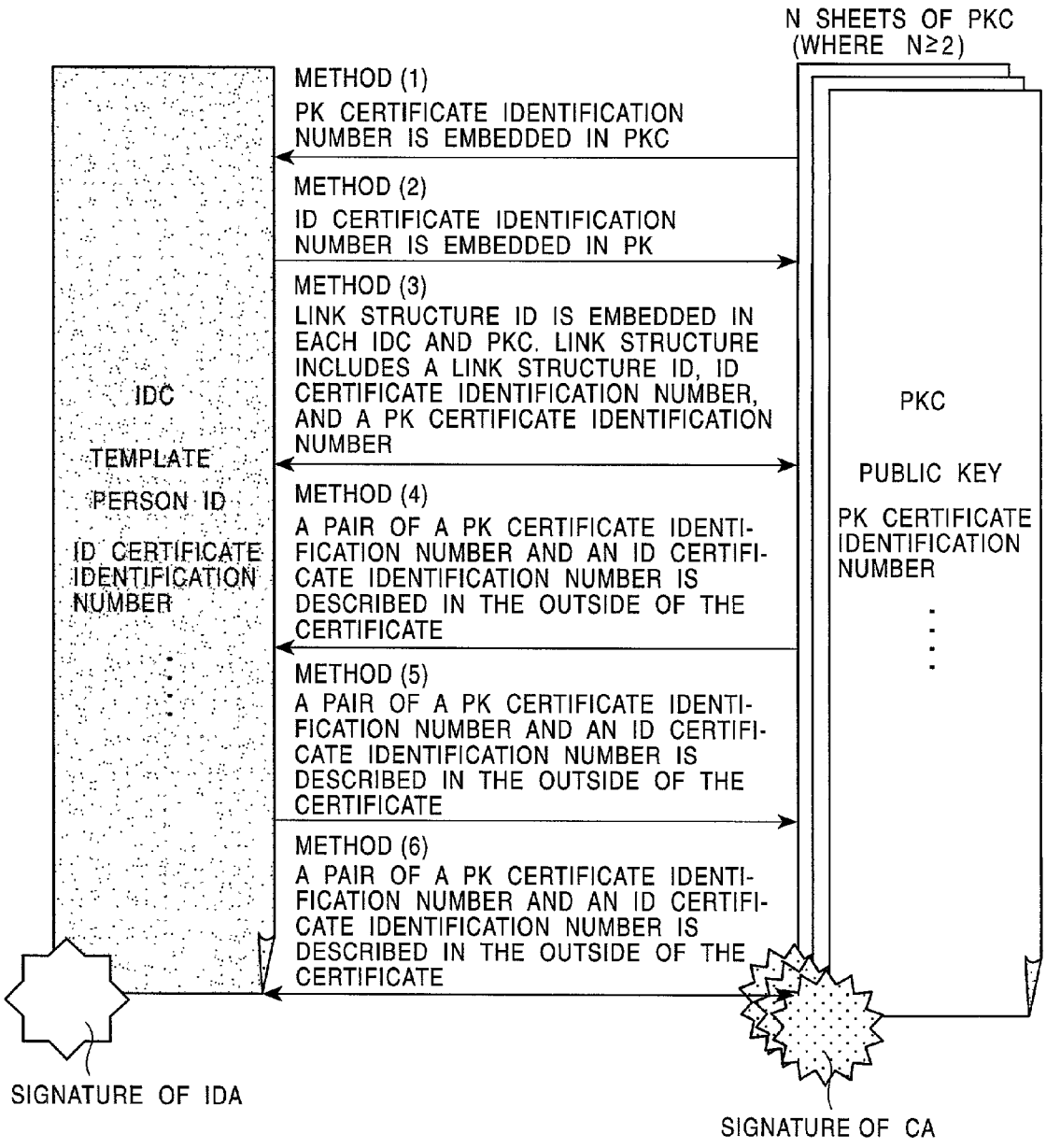

N SHEETS OF PKC
(WHERE N≥2)
METHOD (1)
PK CERTIFICATE IDENTIFICATION NUMBER IS EMBEDDED IN PKC
METHOD (2)
ID CERTIFICATE IDENTIFICATION NUMBER IS EMBEDDED IN PK
METHOD (3)
LINK STRUCTURE ID IS EMBEDDED IN EACH IDC AND PKC. LINK STRUCTURE INCLUDES A LINK STRUCTURE ID, ID CERTIFICATE IDENTIFICATION NUMBER, AND A PK CERTIFICATE IDENTIFICATION NUMBER
METHOD (4)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (5)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (6)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
IDC
TEMPLATE
PERSON ID
ID CERTIFICATE IDENTIFICATION NUMBER
PKC
PUBLIC KEY
PK CERTIFICATE IDENTIFICATION NUMBER
SIGNATURE OF IDA
SIGNATURE OF CA

FIG. 48A

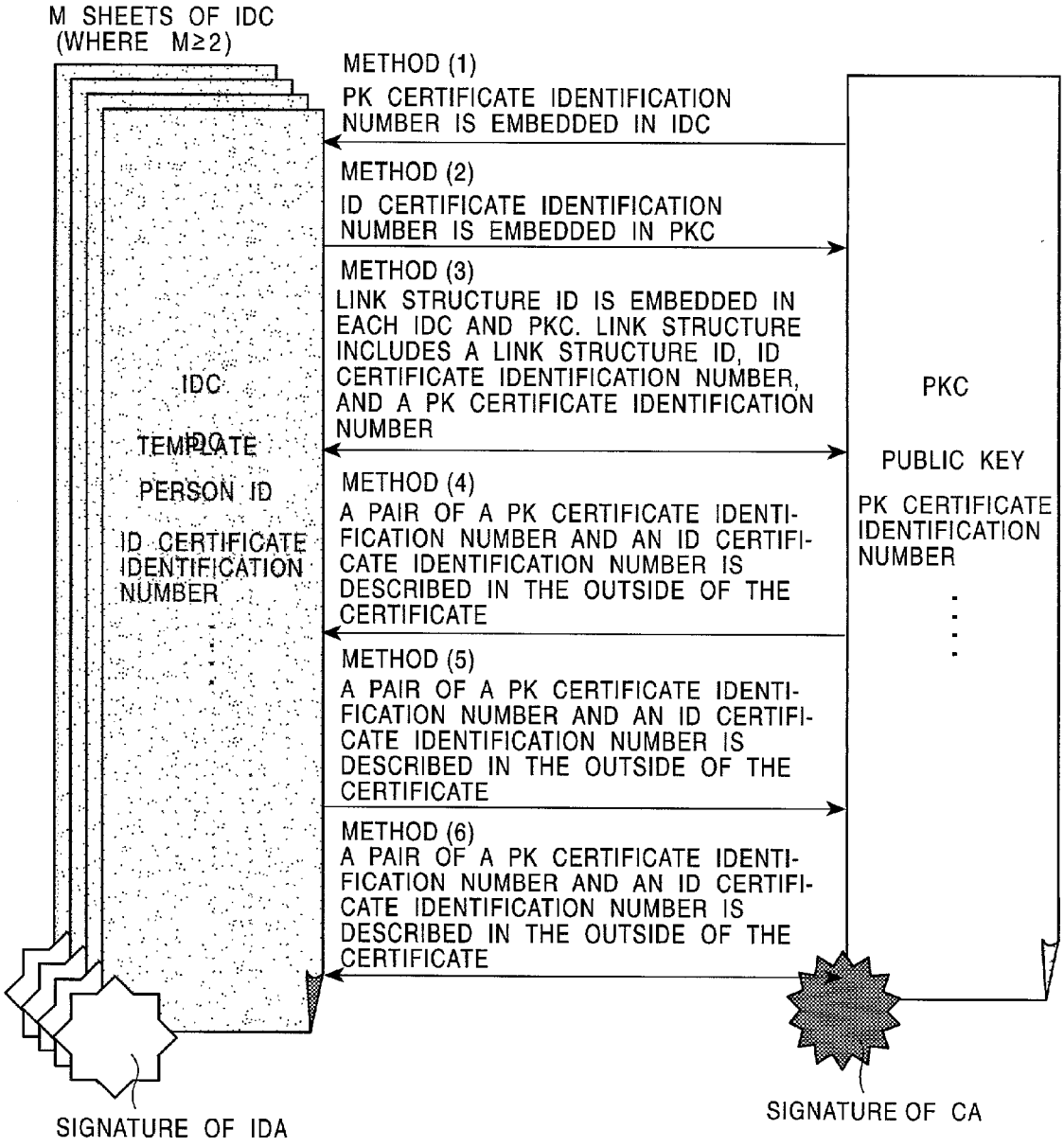

M SHEETS OF IDC
(WHERE M≥2)
IDC
TEMPLATE
PERSON ID
ID CERTIFICATE IDENTIFICATION NUMBER
METHOD (1)
PK CERTIFICATE IDENTIFICATION NUMBER IS EMBEDDED IN IDC
METHOD (2)
ID CERTIFICATE IDENTIFICATION NUMBER IS EMBEDDED IN PKC
METHOD (3)
LINK STRUCTURE ID IS EMBEDDED IN EACH IDC AND PKC. LINK STRUCTURE INCLUDES A LINK STRUCTURE ID, ID CERTIFICATE IDENTIFICATION NUMBER, AND A PK CERTIFICATE IDENTIFICATION NUMBER
METHOD (4)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (5)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (6)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
PKC
PUBLIC KEY
PK CERTIFICATE IDENTIFICATION NUMBER
SIGNATURE OF IDA
SIGNATURE OF CA

FIG. 48B

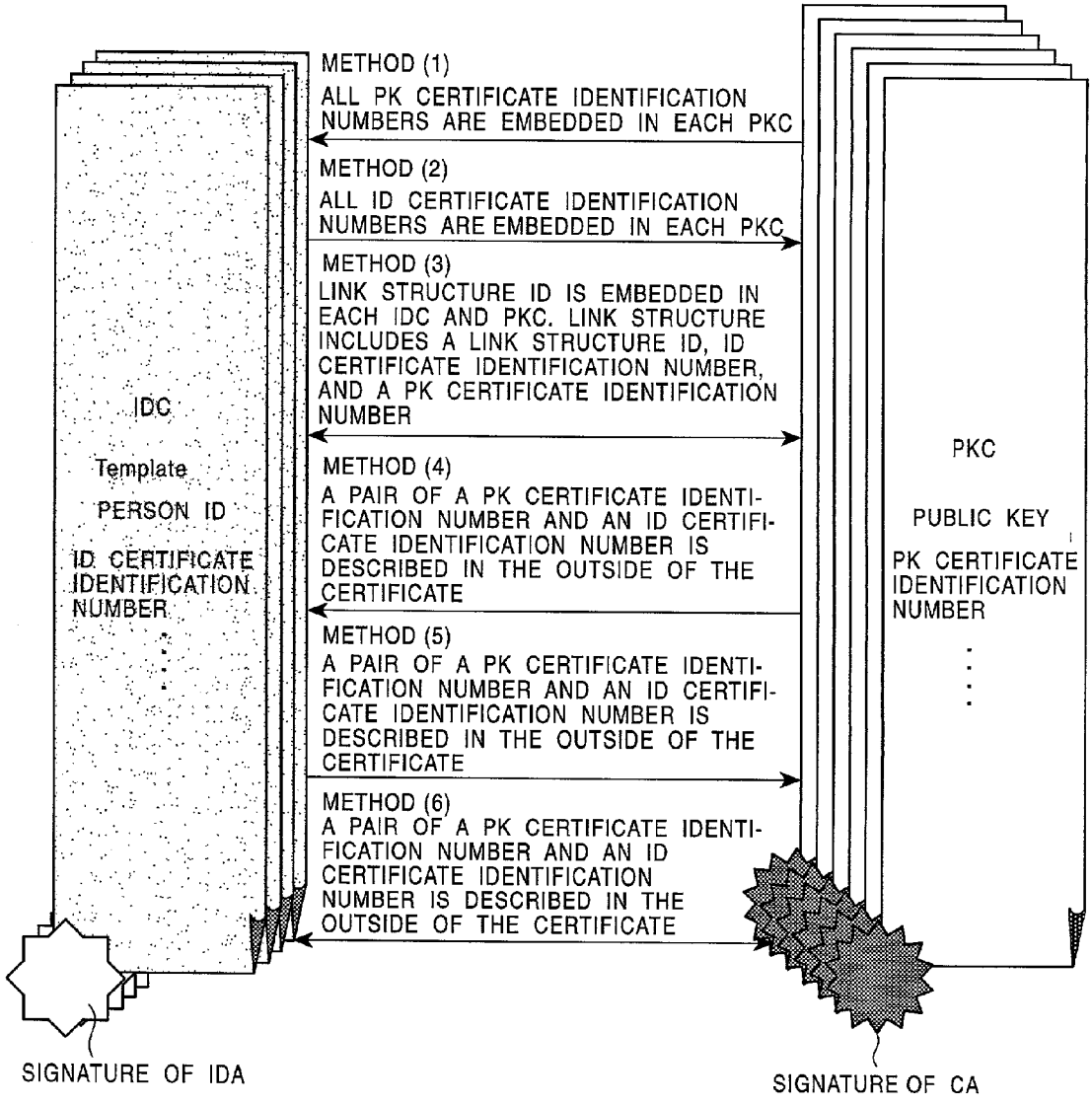

METHOD (1)
ALL PK CERTIFICATE IDENTIFICATION NUMBERS ARE EMBEDDED IN EACH PKC
METHOD (2)
ALL ID CERTIFICATE IDENTIFICATION NUMBERS ARE EMBEDDED IN EACH PKC
METHOD (3)
LINK STRUCTURE ID IS EMBEDDED IN EACH IDC AND PKC. LINK STRUCTURE INCLUDES A LINK STRUCTURE ID, ID CERTIFICATE IDENTIFICATION NUMBER, AND A PK CERTIFICATE IDENTIFICATION NUMBER
METHOD (4)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (5)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (6)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
IDC
Template
PERSON ID
ID CERTIFICATE IDENTIFICATION NUMBER
PKC
PUBLIC KEY
PK CERTIFICATE IDENTIFICATION NUMBER
SIGNATURE OF IDA
SIGNATURE OF CA

FIG. 49A

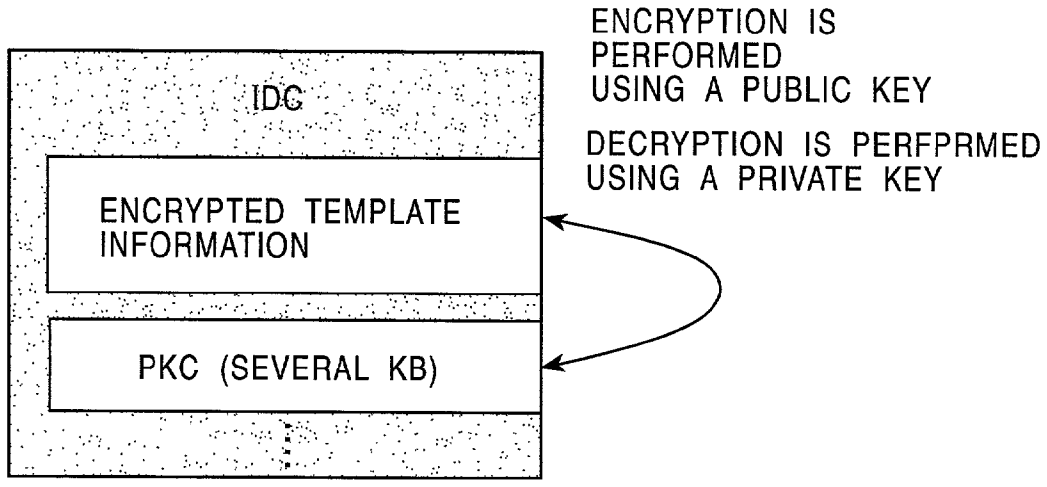


FIG. 49B

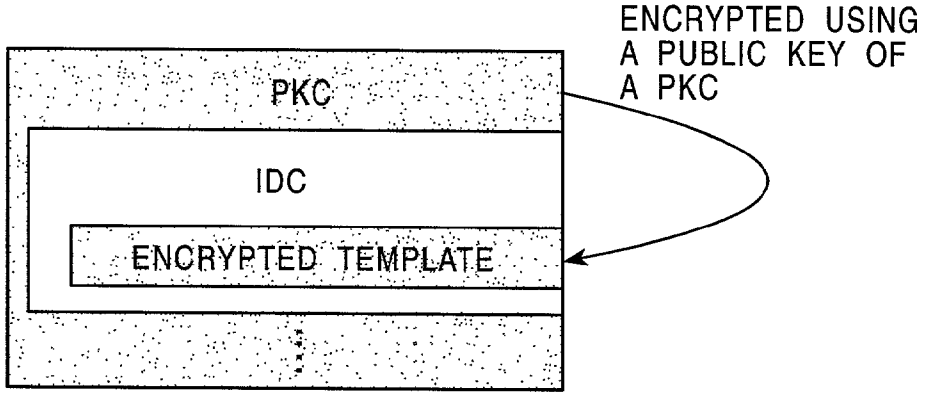


FIG. 50A

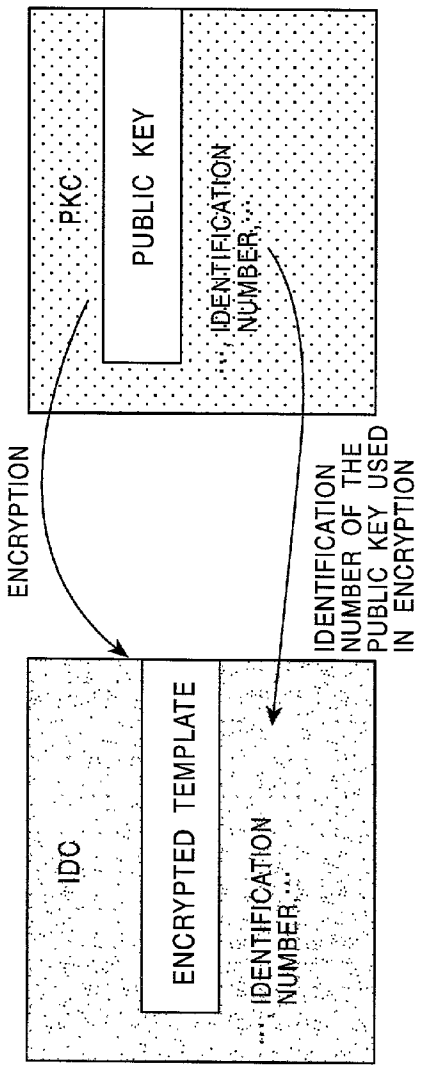
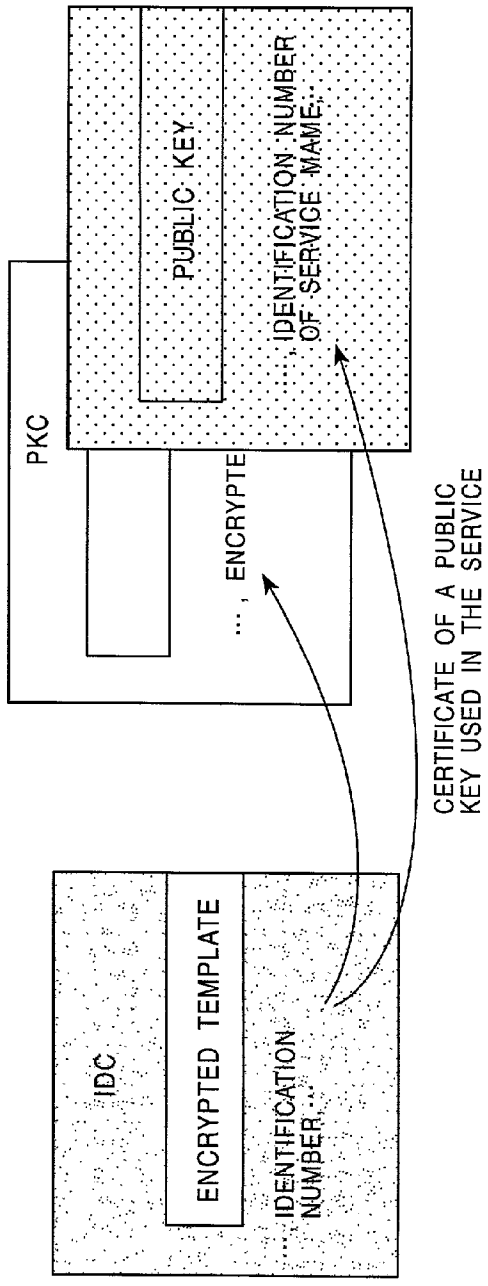


FIG. 50B



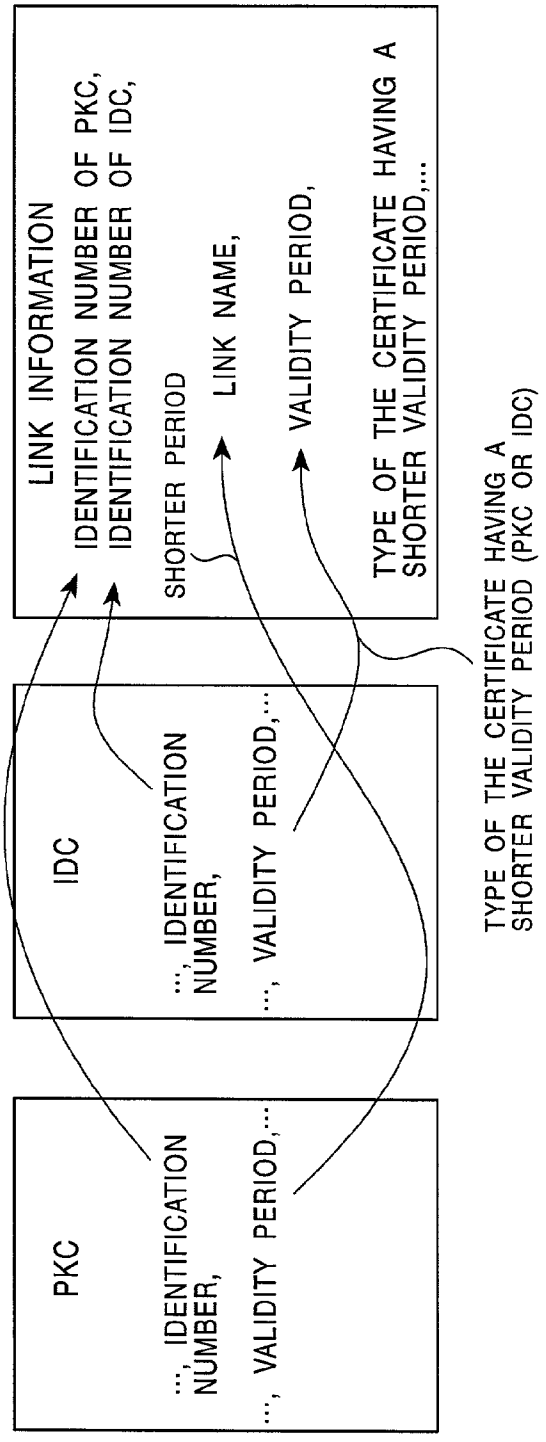


FIG. 51A

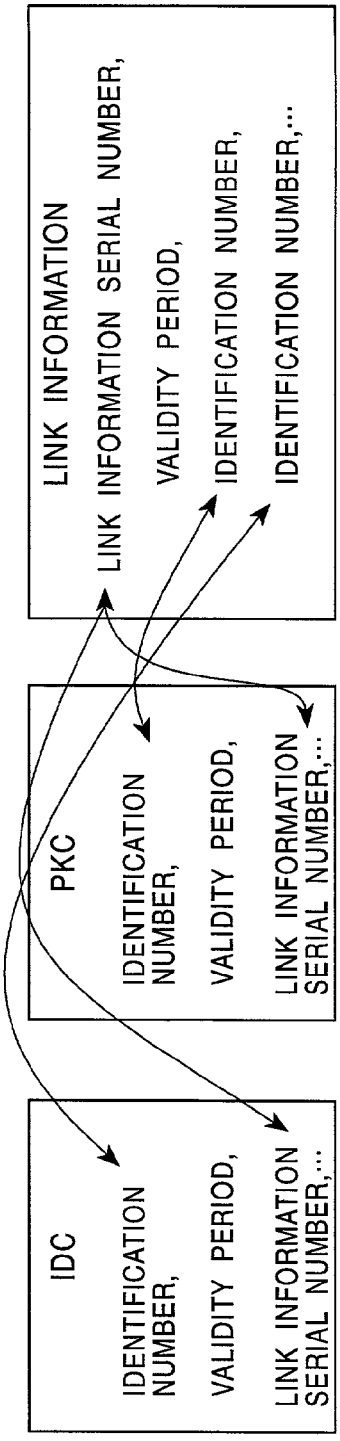


FIG. 51B

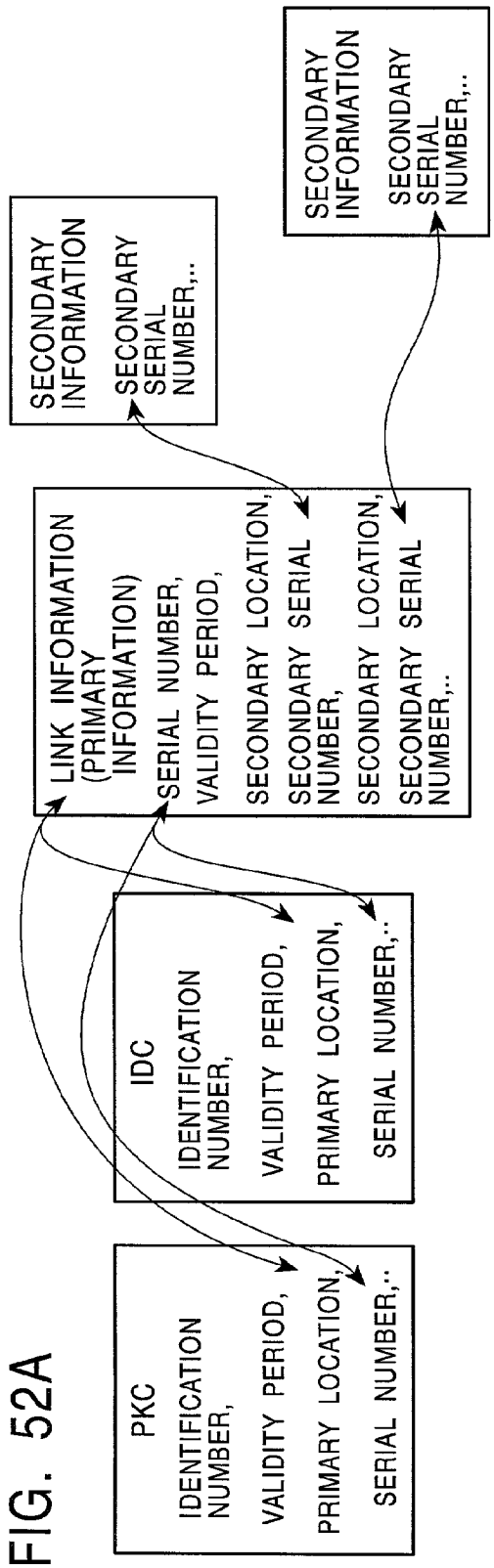


FIG. 52A

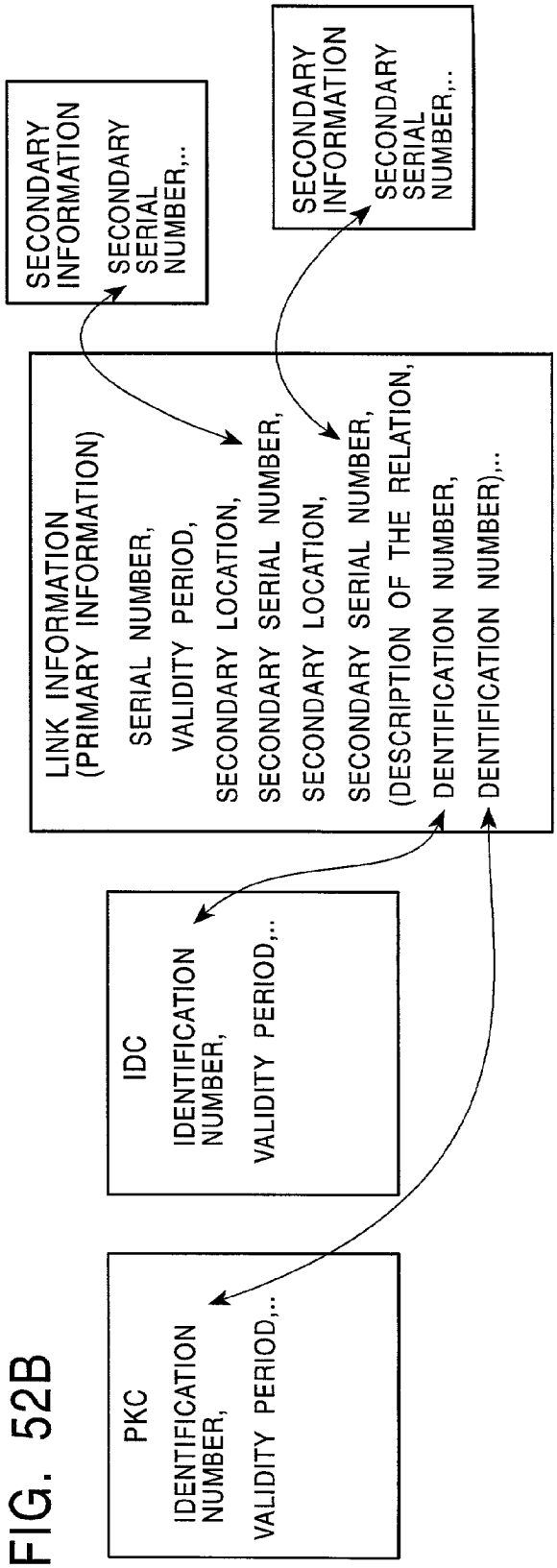


FIG. 52B

FIG. 53

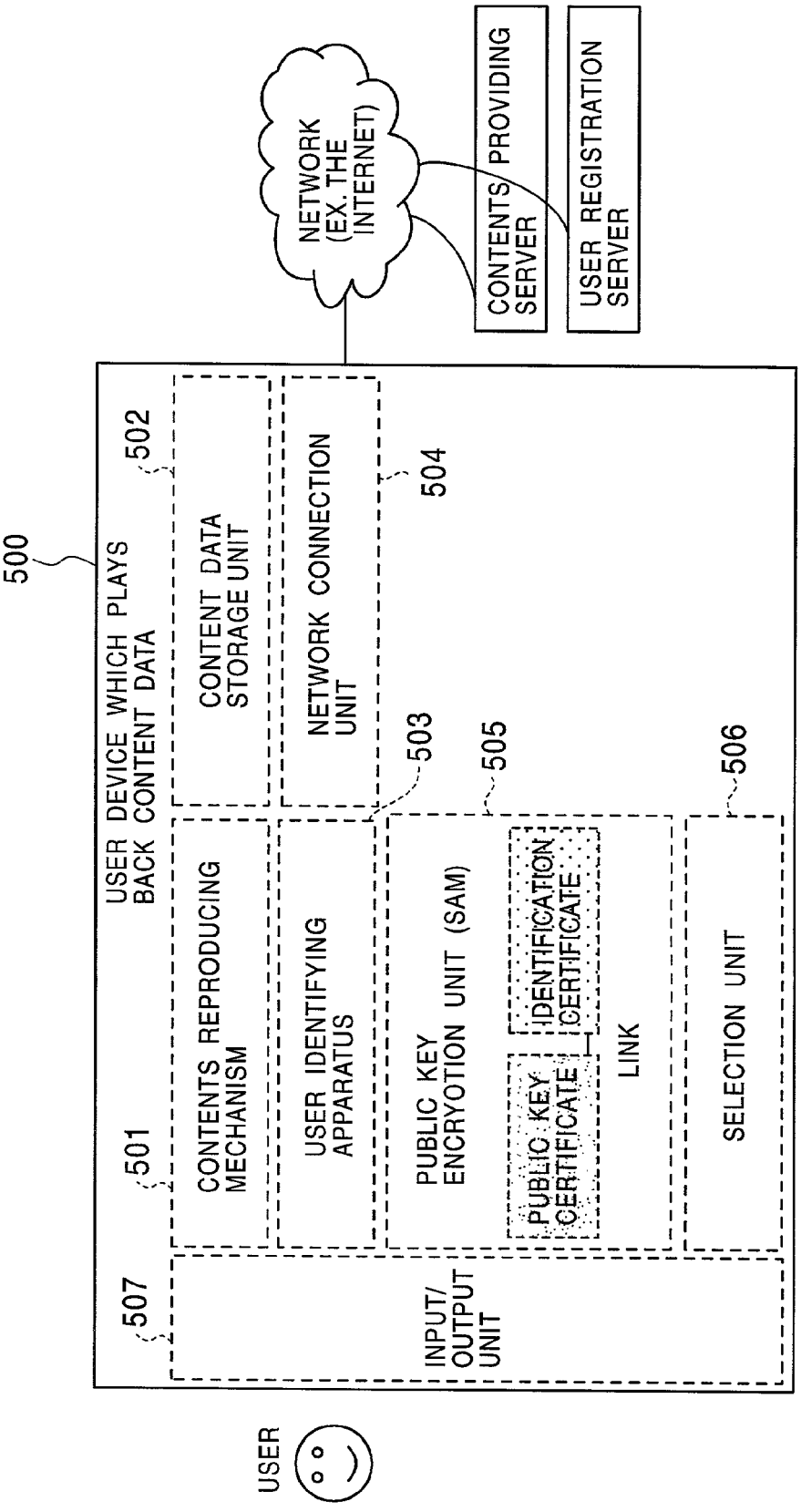

NETWORK (EX. THE INTERNET)
CONTENTS PROVIDING SERVER
USER REGISTRATION SERVER
500
USER DEVICE WHICH PLAYS BACK CONTENT DATA
501
502
503
504
505
506
507
CONTENTS REPRODUCING MECHANISM
CONTENT DATA STORAGE UNIT
USER IDENTIFYING APPARATUS
NETWORK CONNECTION UNIT
PUBLIC KEY ENCRYOTION UNIT (SAM)
PUBLIC KEY CERTIFICATE
IDENTIFICATION CERTIFICATE
LINK
SELECTION UNIT
INPUT/ OUTPUT UNIT
USER

FIG. 54

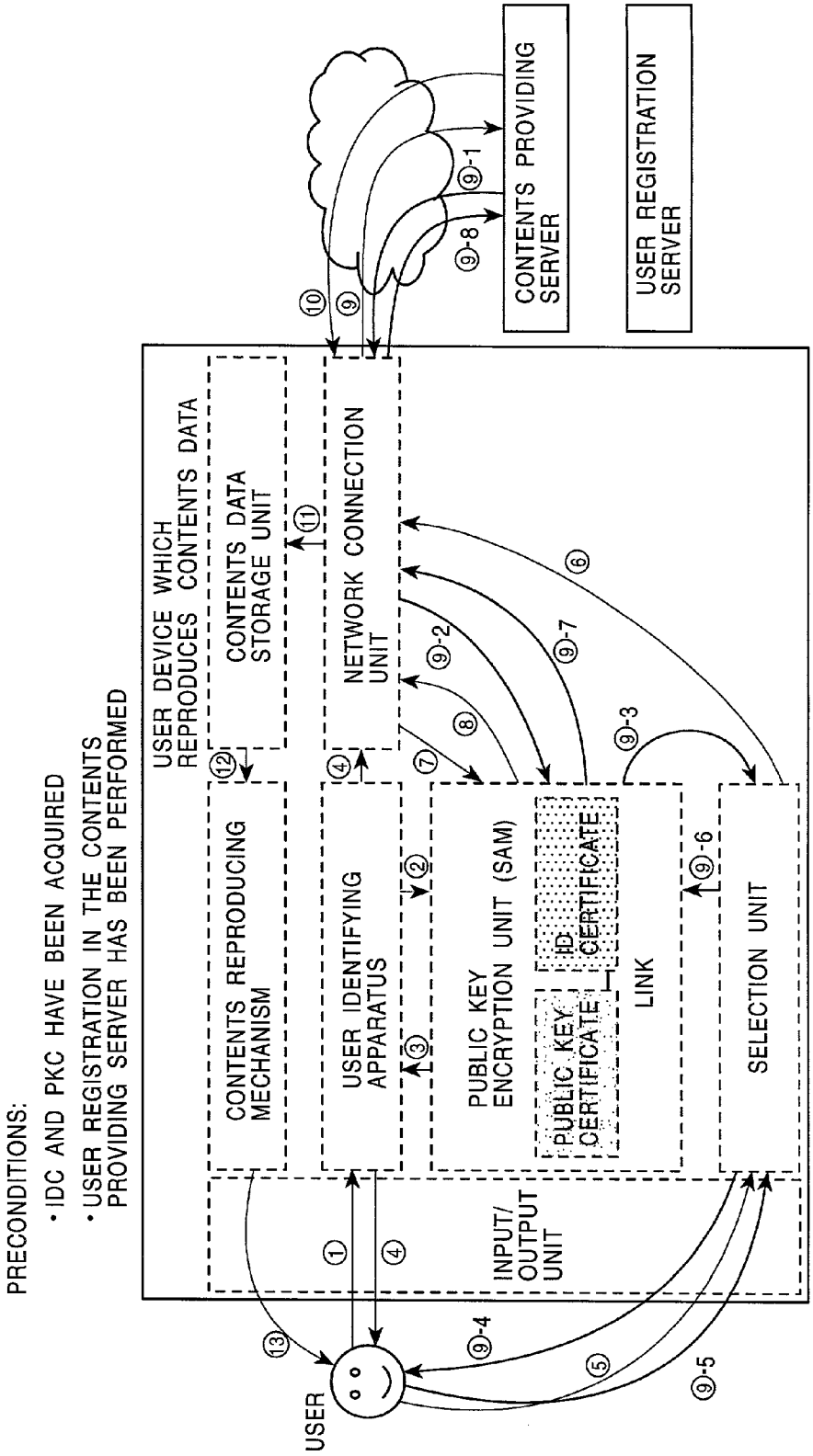

PRECONDITIONS:
• IDC AND PKC HAVE BEEN ACQUIRED
• USER REGISTRATION IN THE CONTENTS PROVIDING SERVER HAS BEEN PERFORMED
USER DEVICE WHICH REPRODUCES CONTENTS DATA
CONTENTS REPRODUCING MECHANISM
CONTENTS DATA STORAGE UNIT
USER IDENTIFYING APPARATUS
NETWORK CONNECTION UNIT
PUBLIC KEY ENCRYPTION UNIT (SAM)
ID CERTIFICATE
PUBLIC KEY CERTIFICATE
LINK
SELECTION UNIT
INPUT/ OUTPUT UNIT
USER
CONTENTS PROVIDING SERVER
USER REGISTRATION SERVER

FIG. 55

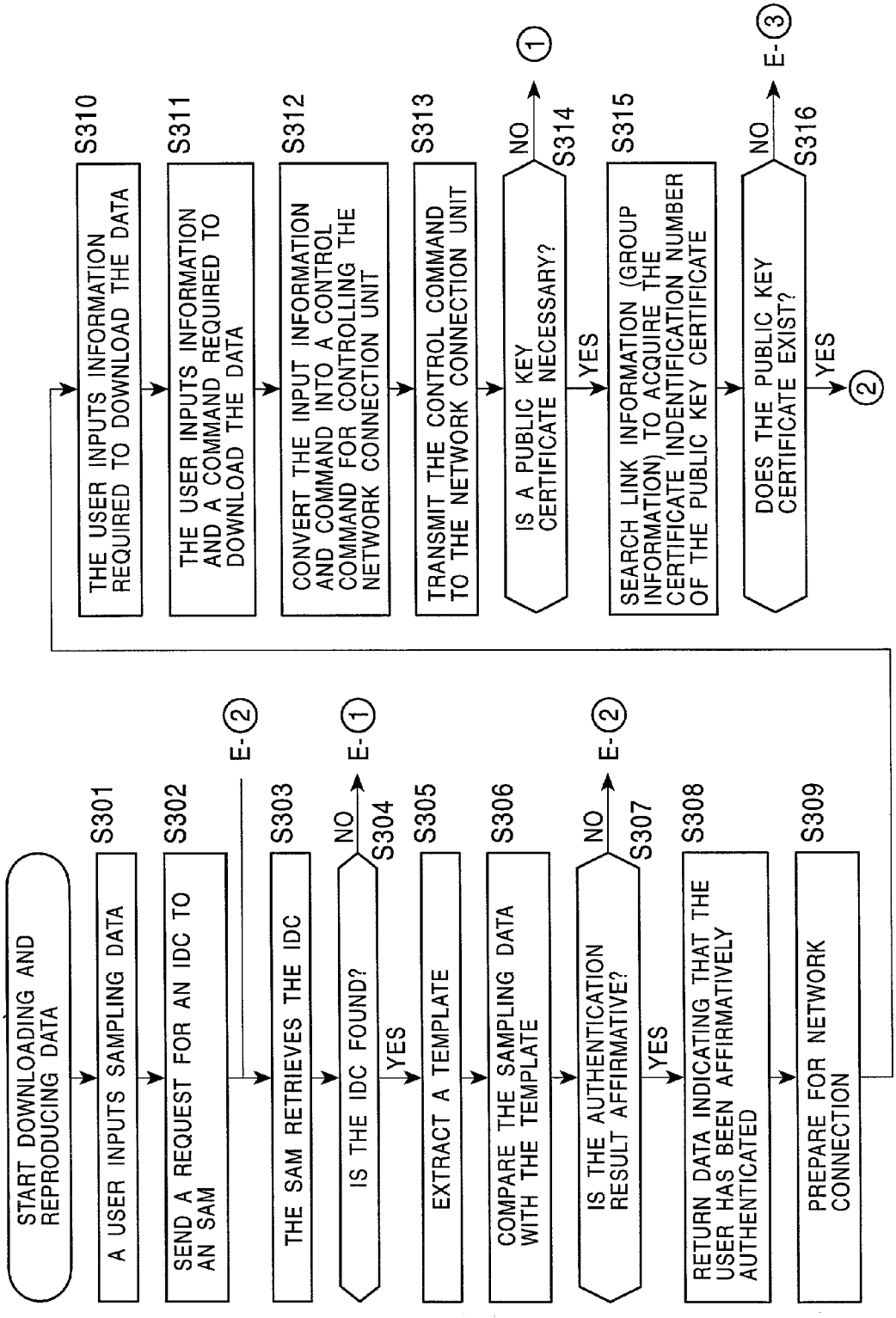

START DOWNLOADING AND REPRODUCING DATA
S301
A USER INPUTS SAMPLING DATA
S302
SEND A REQUEST FOR AN IDC TO AN SAM
E-②
S303
THE SAM RETRIEVES THE IDC
NO
E-①
S304
IS THE IDC FOUND?
YES
S305
EXTRACT A TEMPLATE
S306
COMPARE THE SAMPLING DATA WITH THE TEMPLATE
NO
E-②
S307
IS THE AUTHENTICATION RESULT AFFIRMATIVE?
YES
S308
RETURN DATA INDICATING THAT THE USER HAS BEEN AFFIRMATIVELY AUTHENTICATED
S309
PREPARE FOR NETWORK CONNECTION
S310
THE USER INPUTS INFORMATION REQUIRED TO DOWNLOAD THE DATA
S311
THE USER INPUTS INFORMATION AND A COMMAND REQUIRED TO DOWNLOAD THE DATA
S312
CONVERT THE INPUT INFORMATION AND COMMAND INTO A CONTROL COMMAND FOR CONTROLLING THE NETWORK CONNECTION UNIT
S313
TRANSMIT THE CONTROL COMMAND TO THE NETWORK CONNECTION UNIT
NO
①
S314
IS A PUBLIC KEY CERTIFICATE NECESSARY?
YES
S315
SEARCH LINK INFORMATION (GROUP INFORMATION) TO ACQUIRE THE CERTIFICATE INDENTIFICATION NUMBER OF THE PUBLIC KEY CERTIFICATE
NO
E-③
S316
DOES THE PUBLIC KEY CERTIFICATE EXIST?
YES
②

FIG. 56

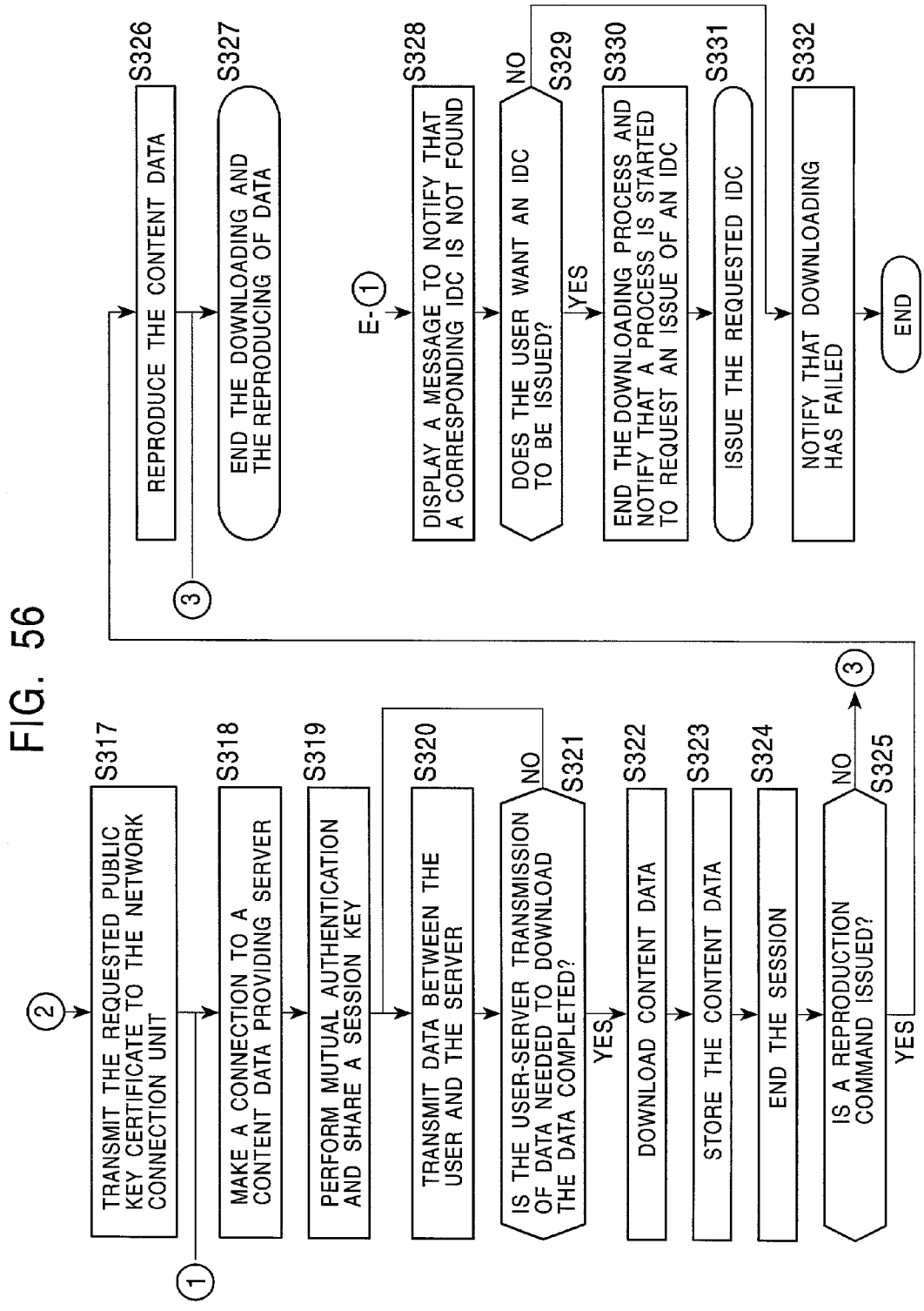

2
S317
TRANSMIT THE REQUESTED PUBLIC KEY CERTIFICATE TO THE NETWORK CONNECTION UNIT
S318
MAKE A CONNECTION TO A CONTENT DATA PROVIDING SERVER
S319
PERFORM MUTUAL AUTHENTICATION AND SHARE A SESSION KEY
S320
TRANSMIT DATA BETWEEN THE USER AND THE SERVER
S321
IS THE USER-SERVER TRANSMISSION OF DATA NEEDED TO DOWNLOAD THE DATA COMPLETED?
NO
YES
S322
DOWNLOAD CONTENT DATA
S323
STORE THE CONTENT DATA
S324
END THE SESSION
S325
IS A REPRODUCTION COMMAND ISSUED?
NO
YES
3
S326
REPRODUCE THE CONTENT DATA
S327
END THE DOWNLOADING AND THE REPRODUCING OF DATA
1
E-1
S328
DISPLAY A MESSAGE TO NOTIFY THAT A CORRESPONDING IDC IS NOT FOUND
S329
DOES THE USER WANT AN IDC TO BE ISSUED?
NO
YES
S330
END THE DOWNLOADING PROCESS AND NOTIFY THAT A PROCESS IS STARTED TO REQUEST AN ISSUE OF AN IDC
S331
ISSUE THE REQUESTED IDC
S332
NOTIFY THAT DOWNLOADING HAS FAILED
END

FIG. 57

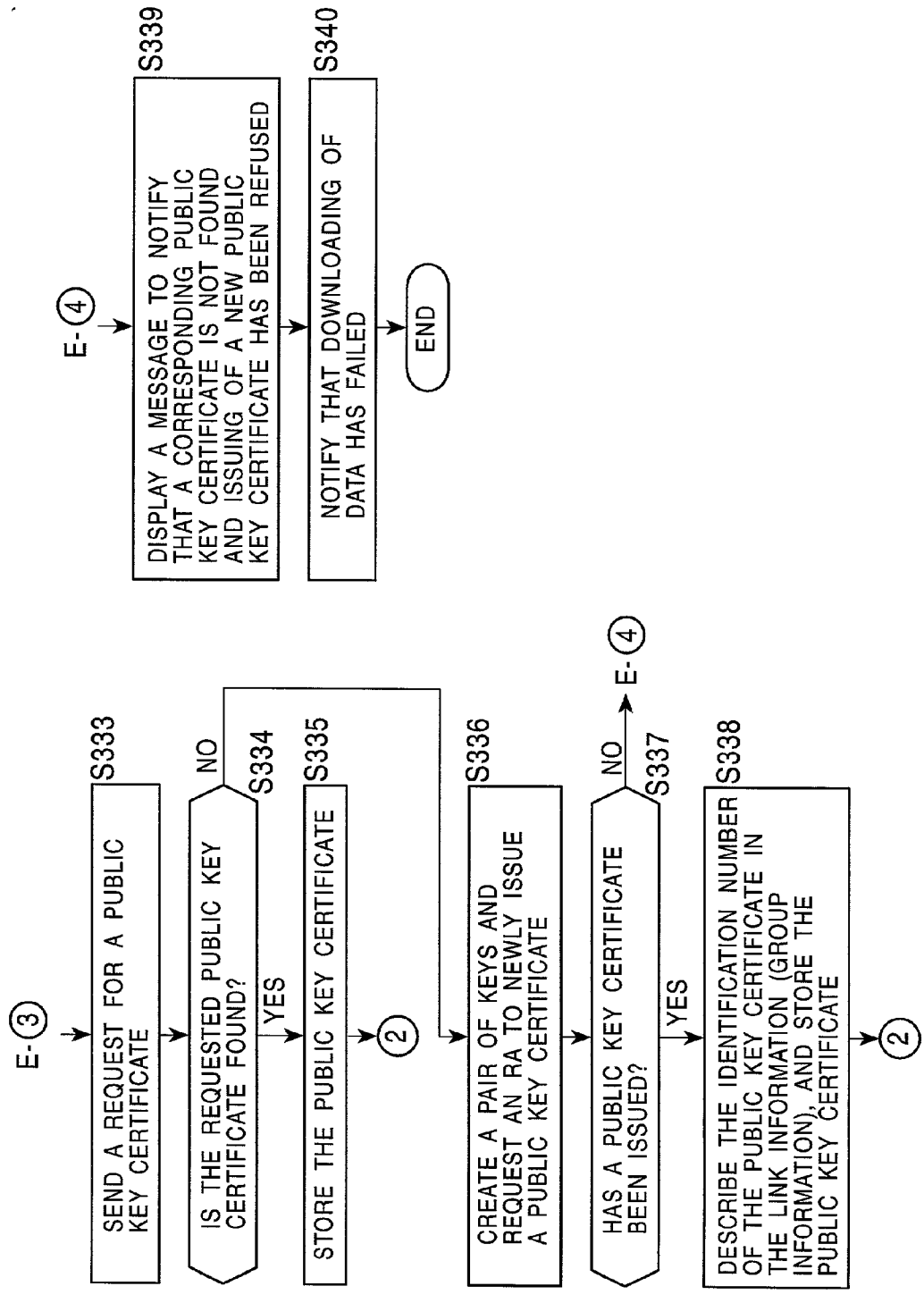

E-3
SEND A REQUEST FOR A PUBLIC KEY CERTIFICATE
S333
IS THE REQUESTED PUBLIC KEY CERTIFICATE FOUND?
S334
NO
YES
STORE THE PUBLIC KEY CERTIFICATE
S335
2
CREATE A PAIR OF KEYS AND REQUEST AN RA TO NEWLY ISSUE A PUBLIC KEY CERTIFICATE
S336
HAS A PUBLIC KEY CERTIFICATE BEEN ISSUED?
S337
NO
E-4
YES
DESCRIBE THE IDENTIFICATION NUMBER OF THE PUBLIC KEY CERTIFICATE IN THE LINK INFORMATION (GROUP INFORMATION), AND STORE THE PUBLIC KEY CERTIFICATE
S338
2
E-4
DISPLAY A MESSAGE TO NOTIFY THAT A CORRESPONDING PUBLIC KEY CERTIFICATE IS NOT FOUND AND ISSUING OF A NEW PUBLIC KEY CERTIFICATE HAS BEEN REFUSED
S339
NOTIFY THAT DOWNLOADING OF DATA HAS FAILED
S340
END

FIG. 58

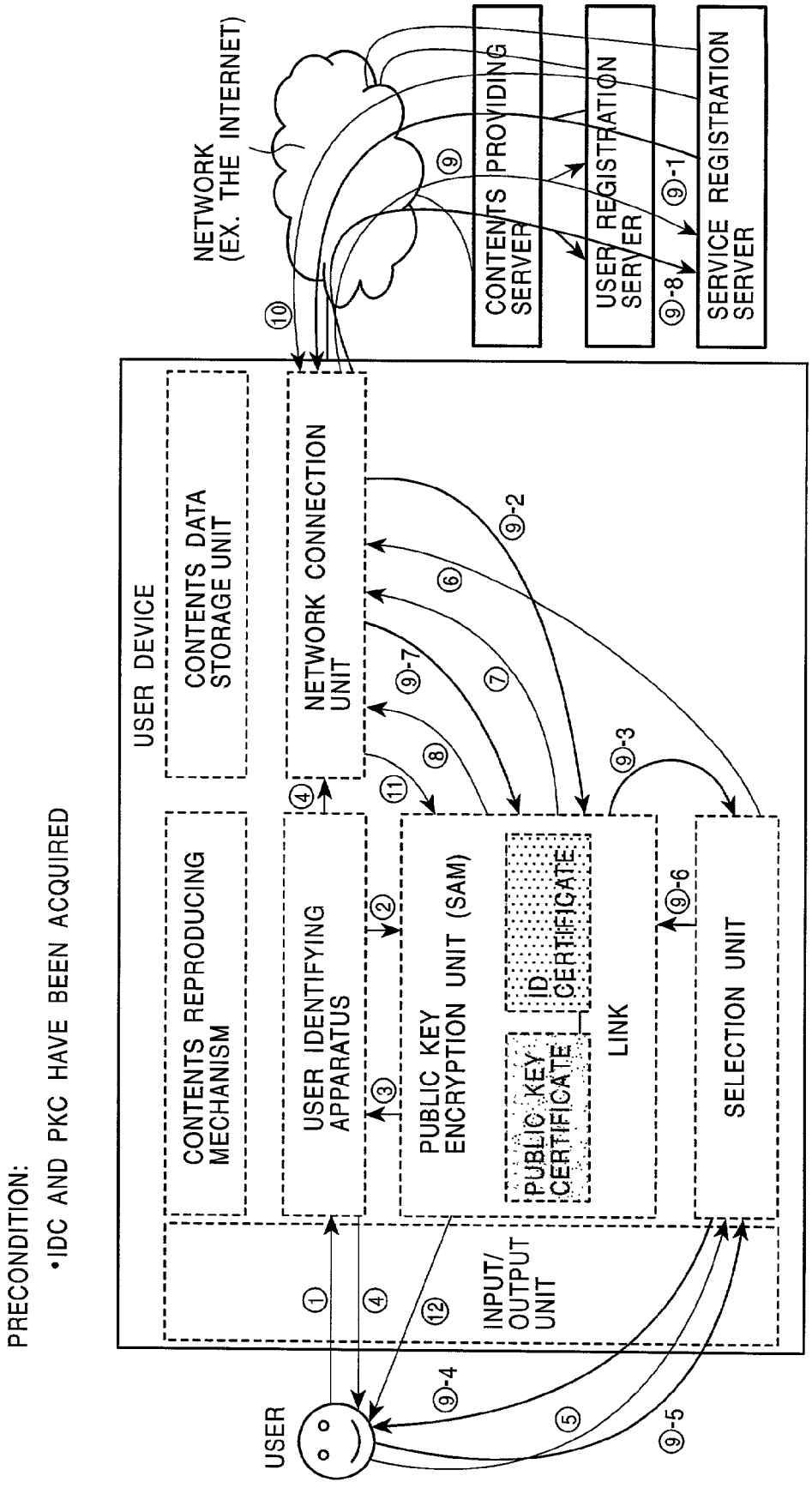

PRECONDITION:
•IDC AND PKC HAVE BEEN ACQUIRED
USER
USER DEVICE
CONTENTS REPRODUCING MECHANISM
CONTENTS DATA STORAGE UNIT
USER IDENTIFYING APPARATUS
NETWORK CONNECTION UNIT
PUBLIC KEY ENCRYPTION UNIT (SAM)
PUBLIC KEY CERTIFICATE
ID CERTIFICATE
LINK
SELECTION UNIT
INPUT/ OUTPUT UNIT
NETWORK (EX. THE INTERNET)
CONTENTS PROVIDING SERVER
USER REGISTRATION SERVER
SERVICE REGISTRATION SERVER
①
②
③
④
⑤
⑥
⑦
⑧
⑨
⑨-1
⑨-2
⑨-3
⑨-4
⑨-5
⑨-6
⑨-7
⑨-8
⑩
⑪
⑫

FIG. 59

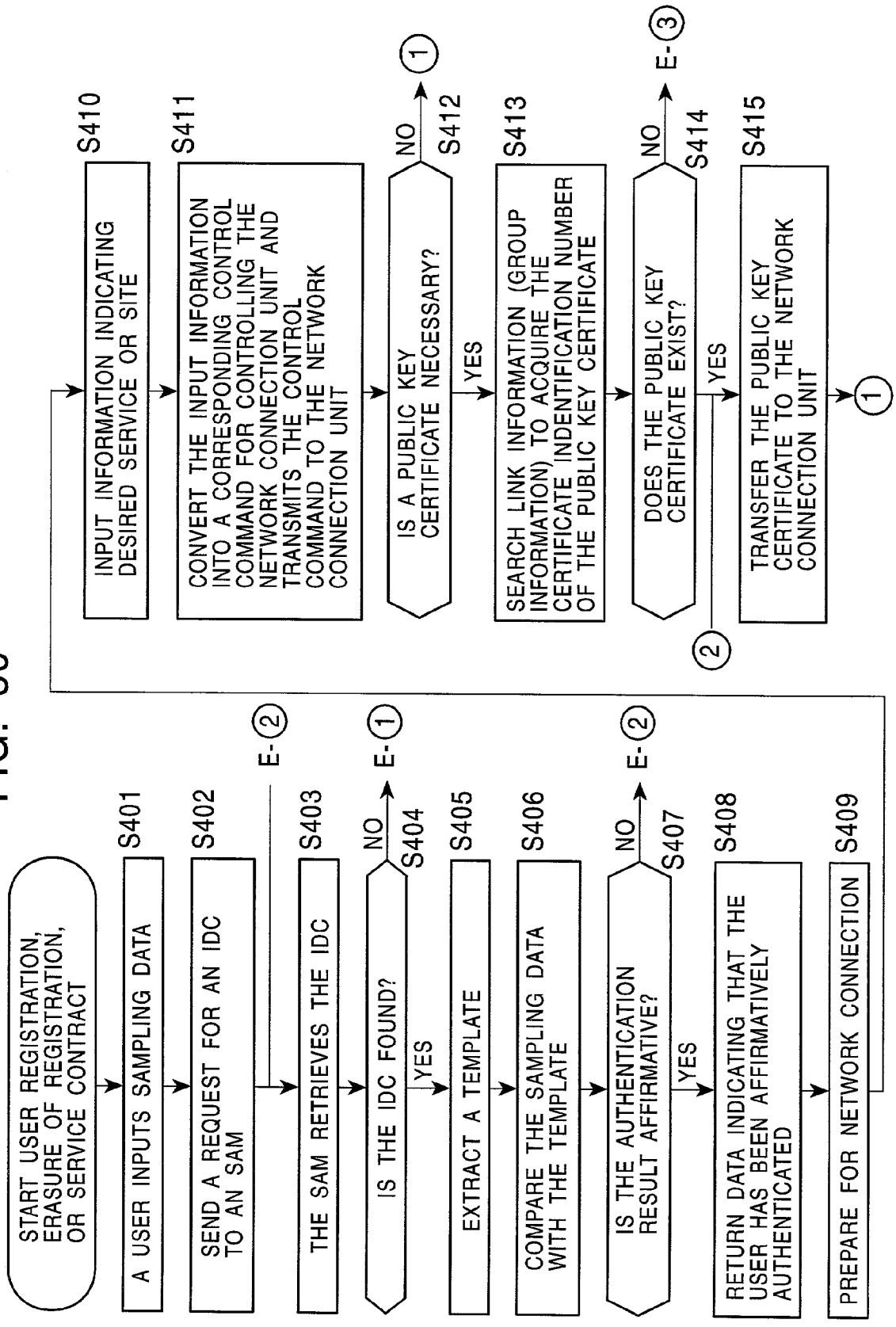

START USER REGISTRATION, ERASURE OF REGISTRATION, OR SERVICE CONTRACT
S401
A USER INPUTS SAMPLING DATA
S402
SEND A REQUEST FOR AN IDC TO AN SAM
E-②
S403
THE SAM RETRIEVES THE IDC
E-①
NO
S404
IS THE IDC FOUND?
YES
S405
EXTRACT A TEMPLATE
S406
COMPARE THE SAMPLING DATA WITH THE TEMPLATE
E-②
NO
S407
IS THE AUTHENTICATION RESULT AFFIRMATIVE?
YES
S408
RETURN DATA INDICATING THAT THE USER HAS BEEN AFFIRMATIVELY AUTHENTICATED
S409
PREPARE FOR NETWORK CONNECTION
S410
INPUT INFORMATION INDICATING DESIRED SERVICE OR SITE
S411
CONVERT THE INPUT INFORMATION INTO A CORRESPONDING CONTROL COMMAND FOR CONTROLLING THE NETWORK CONNECTION UNIT AND TRANSMITS THE CONTROL COMMAND TO THE NETWORK CONNECTION UNIT
①
NO
S412
IS A PUBLIC KEY CERTIFICATE NECESSARY?
YES
S413
SEARCH LINK INFORMATION (GROUP INFORMATION) TO ACQUIRE THE CERTIFICATE INDENTIFICATION NUMBER OF THE PUBLIC KEY CERTIFICATE
E-③
NO
S414
DOES THE PUBLIC KEY CERTIFICATE EXIST?
②
YES
S415
TRANSFER THE PUBLIC KEY CERTIFICATE TO THE NETWORK CONNECTION UNIT
①

FIG. 60

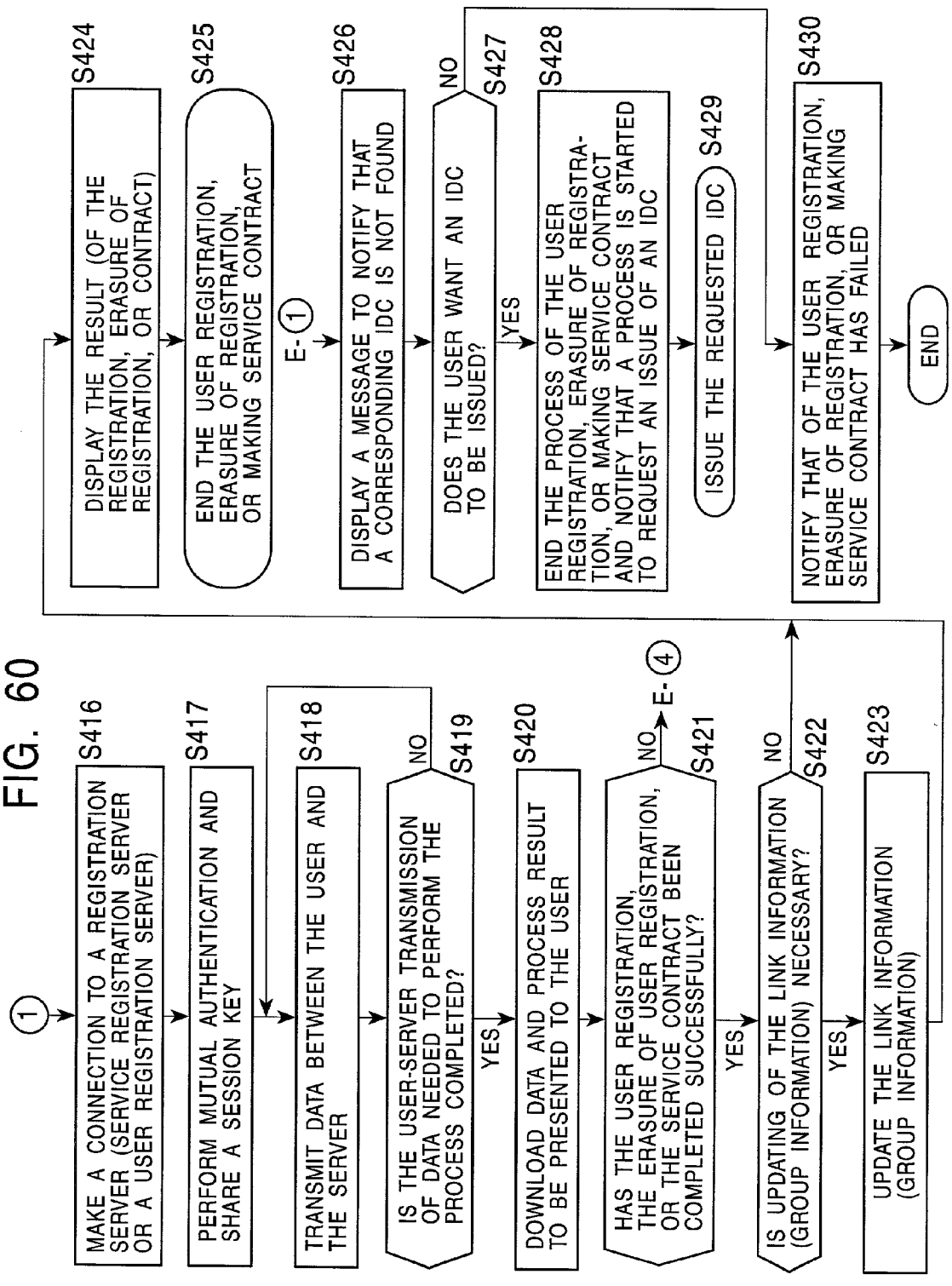

①
MAKE A CONNECTION TO A REGISTRATION SERVER (SERVICE REGISTRATION SERVER OR A USER REGISTRATION SERVER)
S416
PERFORM MUTUAL AUTHENTICATION AND SHARE A SESSION KEY
S417
TRANSMIT DATA BETWEEN THE USER AND THE SERVER
S418
IS THE USER-SERVER TRANSMISSION OF DATA NEEDED TO PERFORM THE PROCESS COMPLETED?
S419
NO
YES
DOWNLOAD DATA AND PROCESS RESULT TO BE PRESENTED TO THE USER
S420
HAS THE USER REGISTRATION, THE ERASURE OF USER REGISTRATION, OR THE SERVICE CONTRACT BEEN COMPLETED SUCCESSFULLY?
S421
NO
E-④
YES
IS UPDATING OF THE LINK INFORMATION (GROUP INFORMATION) NECESSARY?
S422
NO
YES
UPDATE THE LINK INFORMATION (GROUP INFORMATION)
S423
DISPLAY THE RESULT (OF THE REGISTRATION, ERASURE OF REGISTRATION, OR CONTRACT)
S424
END THE USER REGISTRATION, ERASURE OF REGISTRATION, OR MAKING SERVICE CONTRACT
S425
E-①
DISPLAY A MESSAGE TO NOTIFY THAT A CORRESPONDING IDC IS NOT FOUND
S426
DOES THE USER WANT AN IDC TO BE ISSUED?
S427
NO
YES
END THE PROCESS OF THE USER REGISTRATION, ERASURE OF REGISTRATION, OR MAKING SERVICE CONTRACT AND NOTIFY THAT A PROCESS IS STARTED TO REQUEST AN ISSUE OF AN IDC
S428
ISSUE THE REQUESTED IDC
S429
NOTIFY THAT OF THE USER REGISTRATION, ERASURE OF REGISTRATION, OR MAKING SERVICE CONTRACT HAS FAILED
S430
END

FIG. 61

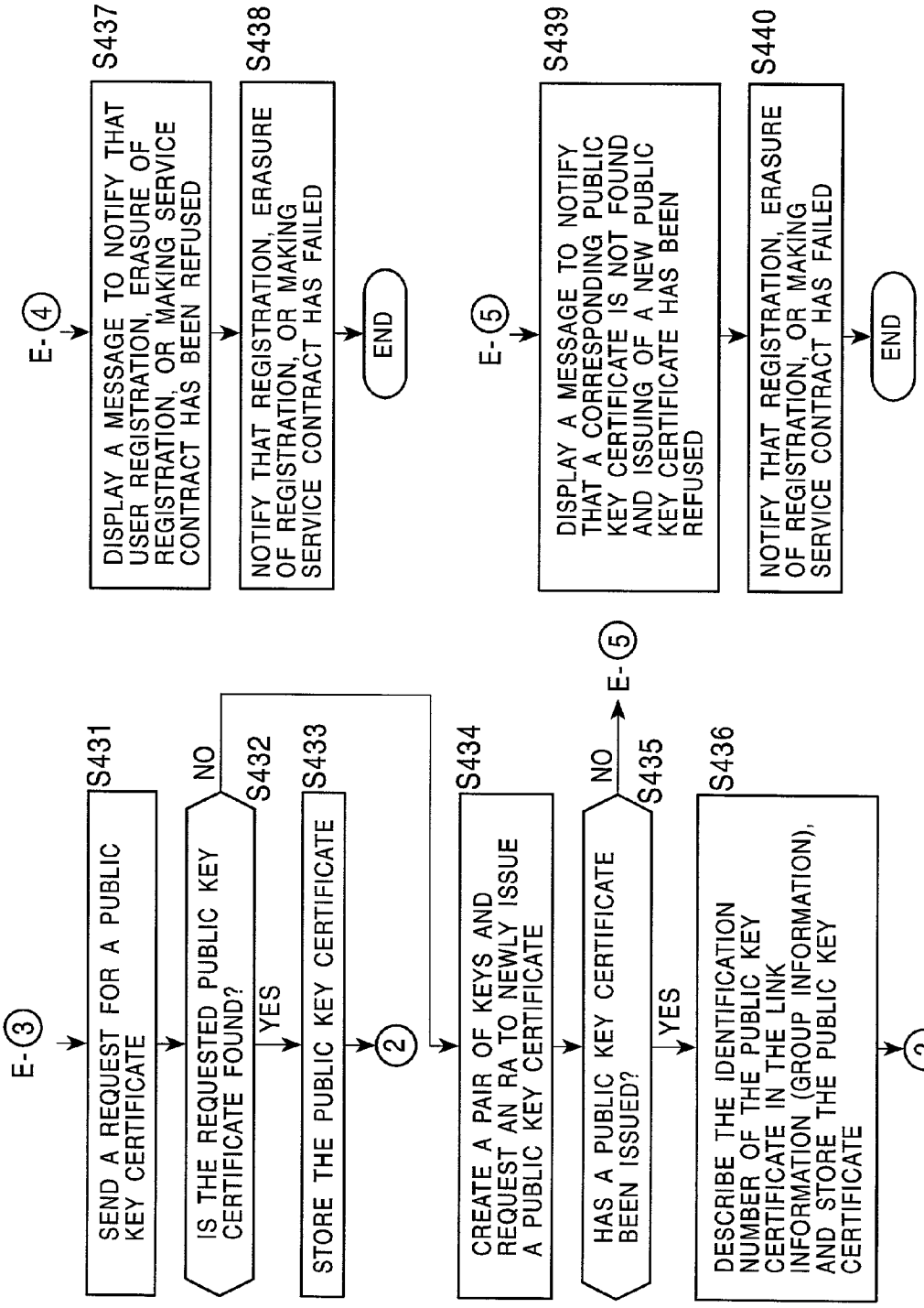

E-3
SEND A REQUEST FOR A PUBLIC KEY CERTIFICATE
S431
IS THE REQUESTED PUBLIC KEY CERTIFICATE FOUND?
S432
NO
YES
STORE THE PUBLIC KEY CERTIFICATE
S433
2
CREATE A PAIR OF KEYS AND REQUEST AN RA TO NEWLY ISSUE A PUBLIC KEY CERTIFICATE
S434
HAS A PUBLIC KEY CERTIFICATE BEEN ISSUED?
S435
NO
YES
E-5
DESCRIBE THE IDENTIFICATION NUMBER OF THE PUBLIC KEY CERTIFICATE IN THE LINK INFORMATION (GROUP INFORMATION), AND STORE THE PUBLIC KEY CERTIFICATE
S436
2
E-4
DISPLAY A MESSAGE TO NOTIFY THAT USER REGISTRATION, ERASURE OF REGISTRATION, OR MAKING SERVICE CONTRACT HAS BEEN REFUSED
S437
NOTIFY THAT REGISTRATION, ERASURE OF REGISTRATION, OR MAKING SERVICE CONTRACT HAS FAILED
S438
END
E-5
DISPLAY A MESSAGE TO NOTIFY THAT A CORRESPONDING PUBLIC KEY CERTIFICATE IS NOT FOUND AND ISSUING OF A NEW PUBLIC KEY CERTIFICATE HAS BEEN REFUSED
S439
NOTIFY THAT REGISTRATION, ERASURE OF REGISTRATION, OR MAKING SERVICE CONTRACT HAS FAILED
S440
END

FIG. 62

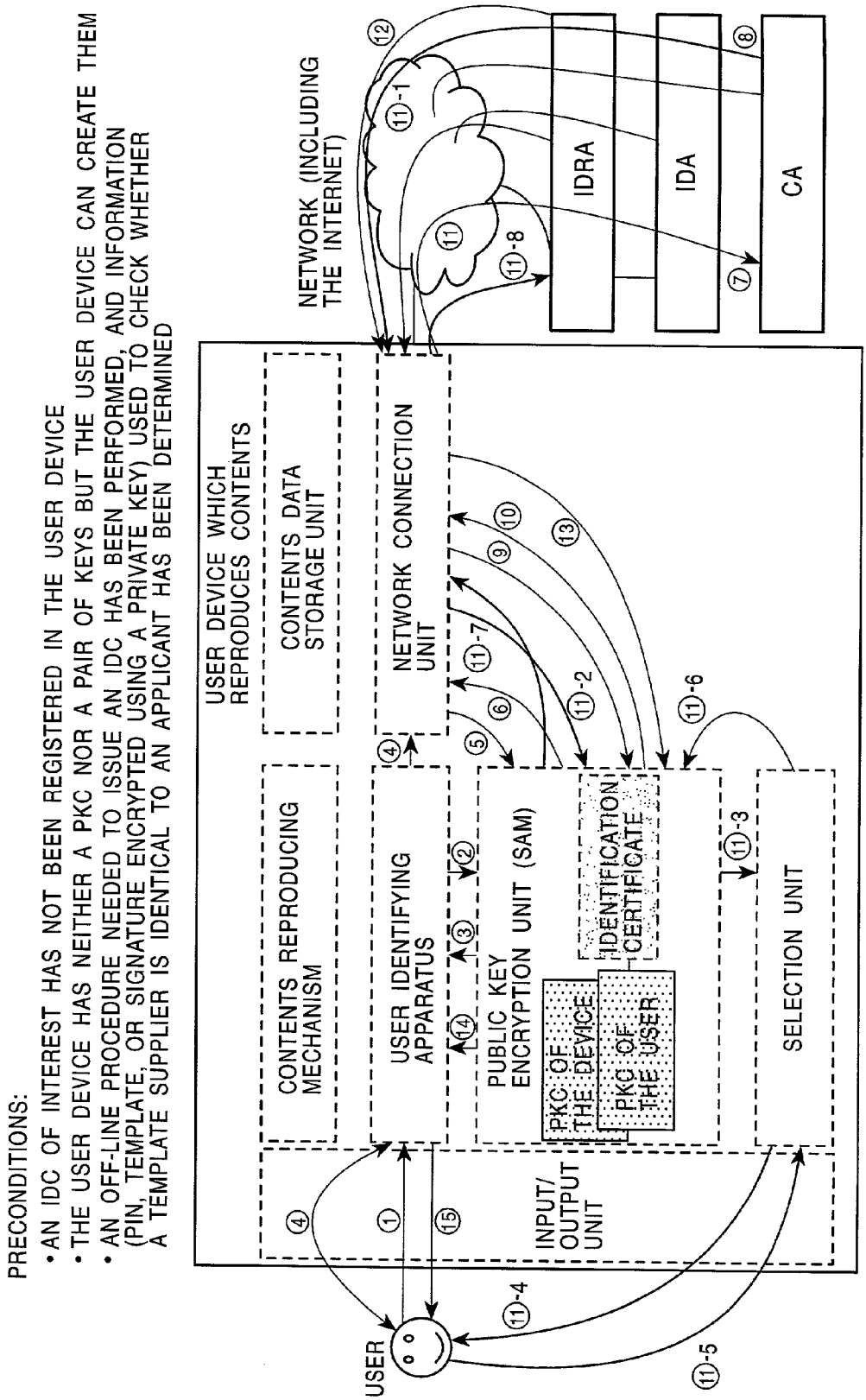

PRECONDITIONS:
• AN IDC OF INTEREST HAS NOT BEEN REGISTERED IN THE USER DEVICE
• THE USER DEVICE HAS NEITHER A PKC NOR A PAIR OF KEYS BUT THE USER DEVICE CAN CREATE THEM
• AN OFF-LINE PROCEDURE NEEDED TO ISSUE AN IDC HAS BEEN PERFORMED, AND INFORMATION (PIN, TEMPLATE, OR SIGNATURE ENCRYPTED USING A PRIVATE KEY) USED TO CHECK WHETHER A TEMPLATE SUPPLIER IS IDENTICAL TO AN APPLICANT HAS BEEN DETERMINED
USER DEVICE WHICH REPRODUCES CONTENTS
CONTENTS REPRODUCING MECHANISM
CONTENTS DATA STORAGE UNIT
USER IDENTIFYING APPARATUS
NETWORK CONNECTION UNIT
PUBLIC KEY ENCRYPTION UNIT (SAM)
PKC OF THE DEVICE
IDENTIFICATION CERTIFICATE
PKC OF THE USER
INPUT/ OUTPUT UNIT
SELECTION UNIT
NETWORK (INCLUDING THE INTERNET)
IDRA
IDA
CA
USER

FIG. 63

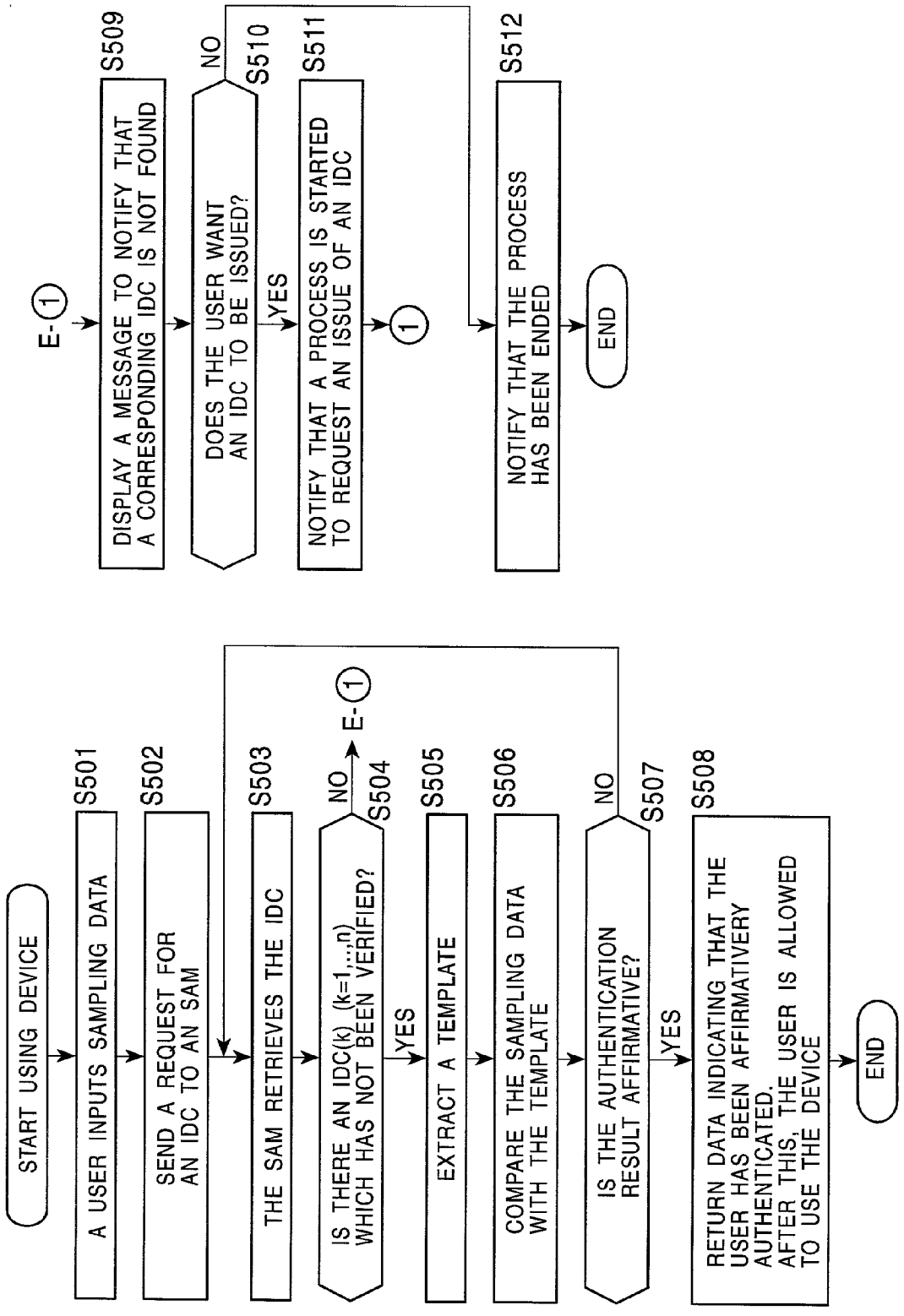

START USING DEVICE
A USER INPUTS SAMPLING DATA
S501
SEND A REQUEST FOR AN IDC TO AN SAM
S502
THE SAM RETRIEVES THE IDC
S503
IS THERE AN IDC(k) (k=1,...,n) WHICH HAS NOT BEEN VERIFIED?
S504
NO
E-1
YES
EXTRACT A TEMPLATE
S505
COMPARE THE SAMPLING DATA WITH THE TEMPLATE
S506
IS THE AUTHENTICATION RESULT AFFIRMATIVE?
S507
NO
YES
RETURN DATA INDICATING THAT THE USER HAS BEEN AFFIRMATIVERY AUTHENTICATED. AFTER THIS, THE USER IS ALLOWED TO USE THE DEVICE
S508
END
E-1
DISPLAY A MESSAGE TO NOTIFY THAT A CORRESPONDING IDC IS NOT FOUND
S509
DOES THE USER WANT AN IDC TO BE ISSUED?
S510
NO
YES
NOTIFY THAT A PROCESS IS STARTED TO REQUEST AN ISSUE OF AN IDC
S511
1
NOTIFY THAT THE PROCESS HAS BEEN ENDED
S512
END

FIG. 64

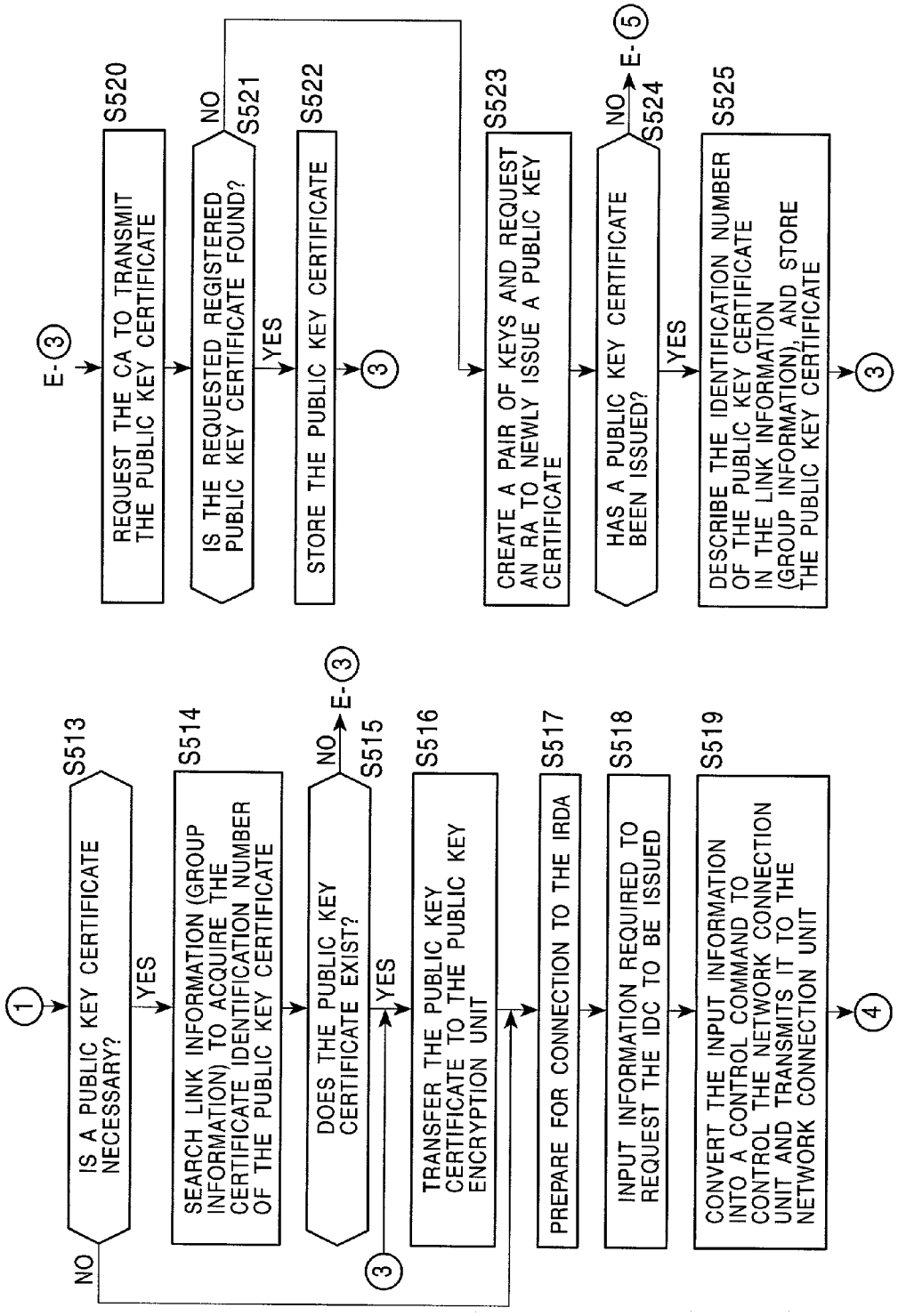

1
IS A PUBLIC KEY CERTIFICATE NECESSARY?
S513
YES
NO
SEARCH LINK INFORMATION (GROUP INFORMATION) TO ACQUIRE THE CERTIFICATE IDENTIFICATION NUMBER OF THE PUBLIC KEY CERTIFICATE
S514
DOES THE PUBLIC KEY CERTIFICATE EXIST?
S515
NO
E-3
YES
3
TRANSFER THE PUBLIC KEY CERTIFICATE TO THE PUBLIC KEY ENCRYPTION UNIT
S516
PREPARE FOR CONNECTION TO THE IRDA
S517
INPUT INFORMATION REQUIRED TO REQUEST THE IDC TO BE ISSUED
S518
CONVERT THE INPUT INFORMATION INTO A CONTROL COMMAND TO CONTROL THE NETWORK CONNECTION UNIT AND TRANSMITS IT TO THE NETWORK CONNECTION UNIT
S519
4
E-3
REQUEST THE CA TO TRANSMIT THE PUBLIC KEY CERTIFICATE
S520
IS THE REQUESTED REGISTERED PUBLIC KEY CERTIFICATE FOUND?
S521
NO
YES
STORE THE PUBLIC KEY CERTIFICATE
S522
3
CREATE A PAIR OF KEYS AND REQUEST AN RA TO NEWLY ISSUE A PUBLIC KEY CERTIFICATE
S523
HAS A PUBLIC KEY CERTIFICATE BEEN ISSUED?
S524
NO
E-5
YES
DESCRIBE THE IDENTIFICATION NUMBER OF THE PUBLIC KEY CERTIFICATE IN THE LINK INFORMATION (GROUP INFORMATION), AND STORE THE PUBLIC KEY CERTIFICATE
S525
3

FIG. 65

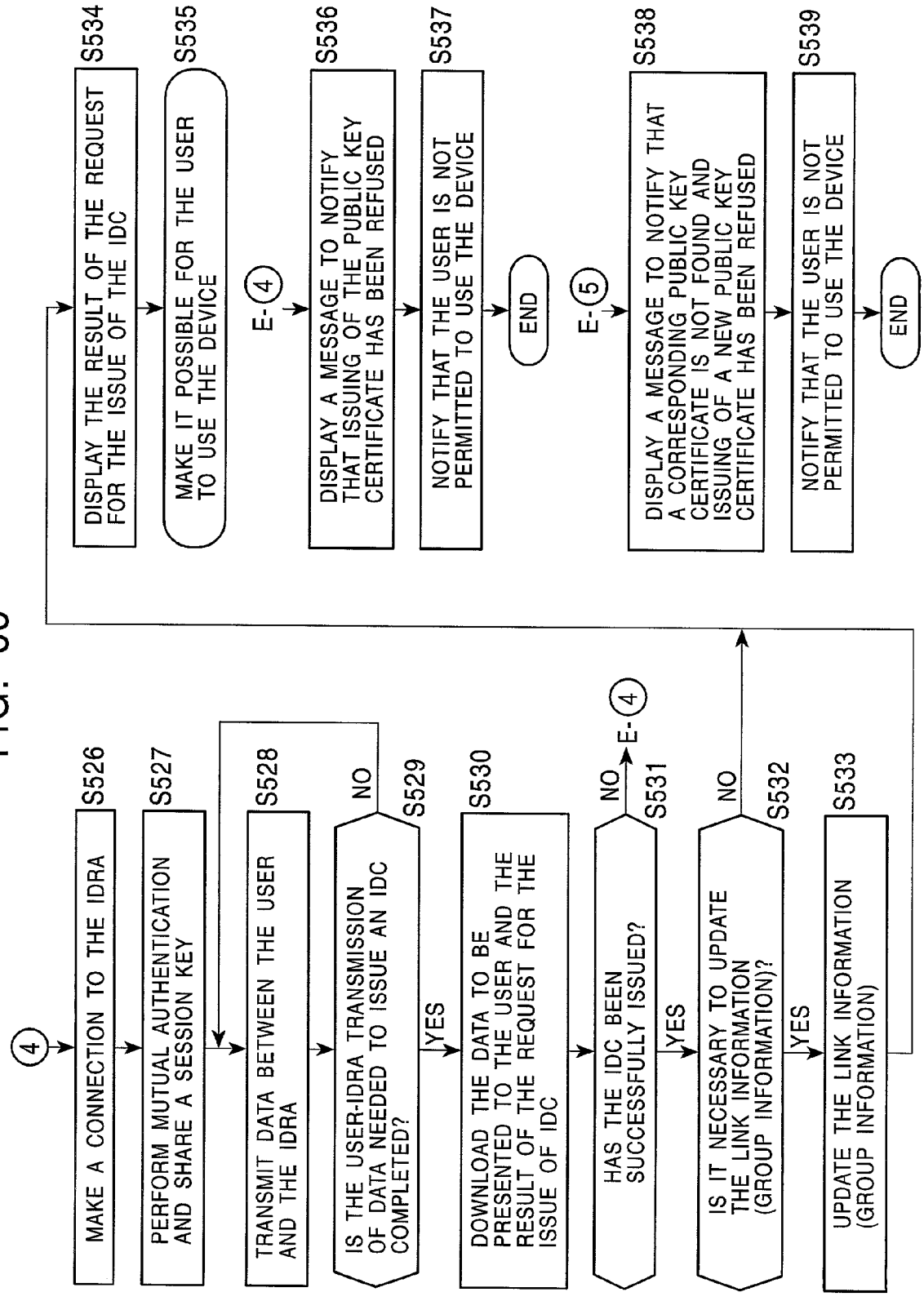

4
MAKE A CONNECTION TO THE IDRA
S526
PERFORM MUTUAL AUTHENTICATION AND SHARE A SESSION KEY
S527
TRANSMIT DATA BETWEEN THE USER AND THE IDRA
S528
IS THE USER-IDRA TRANSMISSION OF DATA NEEDED TO ISSUE AN IDC COMPLETED?
S529
NO
YES
DOWNLOAD THE DATA TO BE PRESENTED TO THE USER AND THE RESULT OF THE REQUEST FOR THE ISSUE OF IDC
S530
HAS THE IDC BEEN SUCCESSFULLY ISSUED?
S531
NO
E-4
YES
IS IT NECESSARY TO UPDATE THE LINK INFORMATION (GROUP INFORMATION)?
S532
NO
YES
UPDATE THE LINK INFORMATION (GROUP INFORMATION)
S533
DISPLAY THE RESULT OF THE REQUEST FOR THE ISSUE OF THE IDC
S534
MAKE IT POSSIBLE FOR THE USER TO USE THE DEVICE
S535
E-4
DISPLAY A MESSAGE TO NOTIFY THAT ISSUING OF THE PUBLIC KEY CERTIFICATE HAS BEEN REFUSED
S536
NOTIFY THAT THE USER IS NOT PERMITTED TO USE THE DEVICE
S537
END
E-5
DISPLAY A MESSAGE TO NOTIFY THAT A CORRESPONDING PUBLIC KEY CERTIFICATE IS NOT FOUND AND ISSUING OF A NEW PUBLIC KEY CERTIFICATE HAS BEEN REFUSED
S538
NOTIFY THAT THE USER IS NOT PERMITTED TO USE THE DEVICE
S539
END

FIG. 66

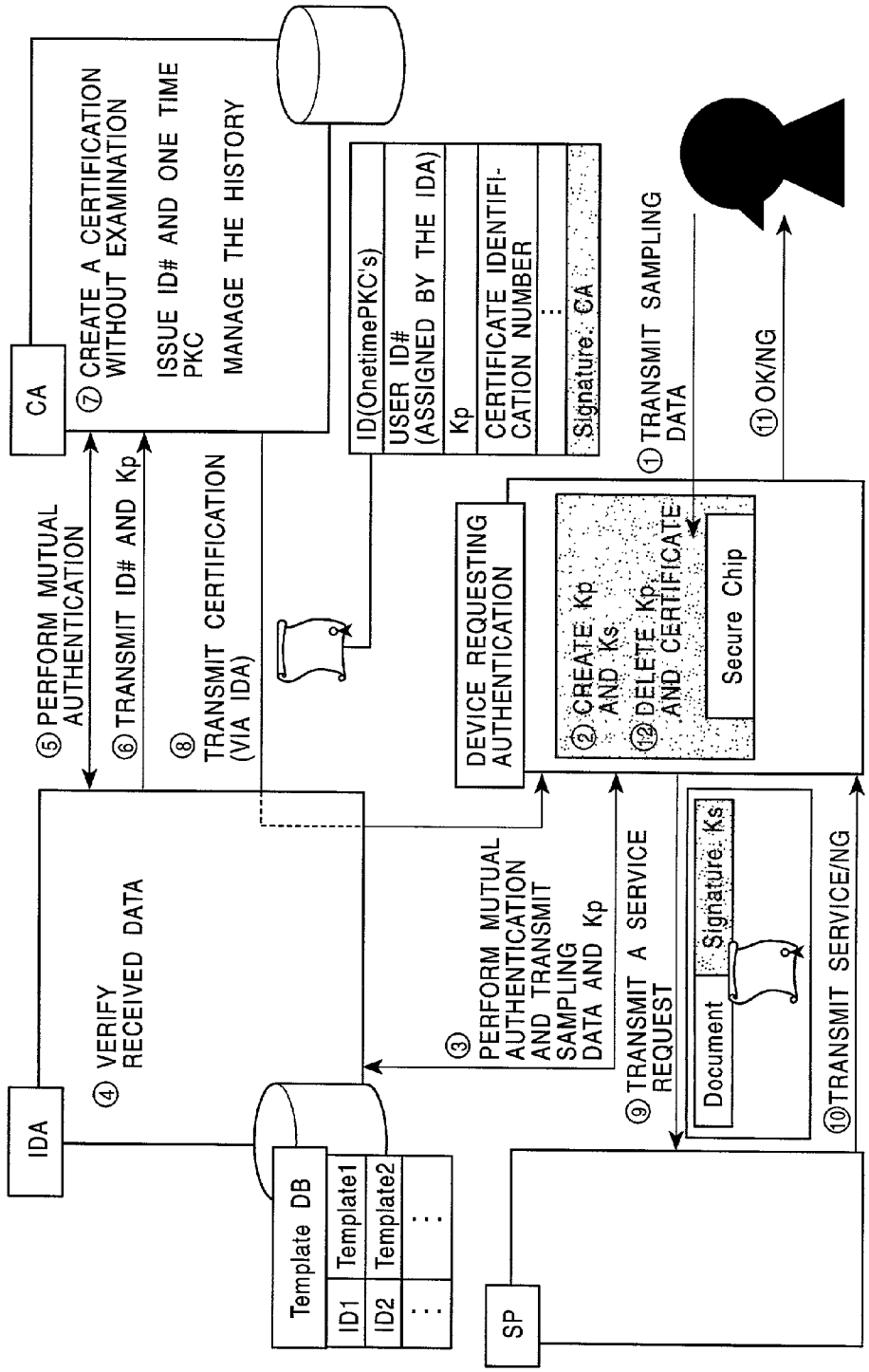

CA
⑦ CREATE A CERTIFICATION WITHOUT EXAMINATION
ISSUE ID# AND ONE TIME PKC
MANAGE THE HISTORY
ID(OnetimePKC's)
USER ID# (ASSIGNED BY THE IDA)
Kp
CERTIFICATE IDENTIFICATION NUMBER
Signature: CA
⑤ PERFORM MUTUAL AUTHENTICATION
⑥ TRANSMIT ID# AND Kp
⑧ TRANSMIT CERTIFICATION (VIA IDA)
① TRANSMIT SAMPLING DATA
⑪ OK/NG
DEVICE REQUESTING AUTHENTICATION
② CREATE Kp AND Ks
⑫ DELETE Kp AND CERTIFICATE
Secure Chip
IDA
④ VERIFY RECEIVED DATA
③ PERFORM MUTUAL AUTHENTICATION AND TRANSMIT SAMPLING DATA AND Kp
⑨ TRANSMIT A SERVICE REQUEST
Document
Signature: Ks
⑩TRANSMIT SERVICE/NG
Template DB
ID1
Template1
ID2
Template2
SP

FIG. 67

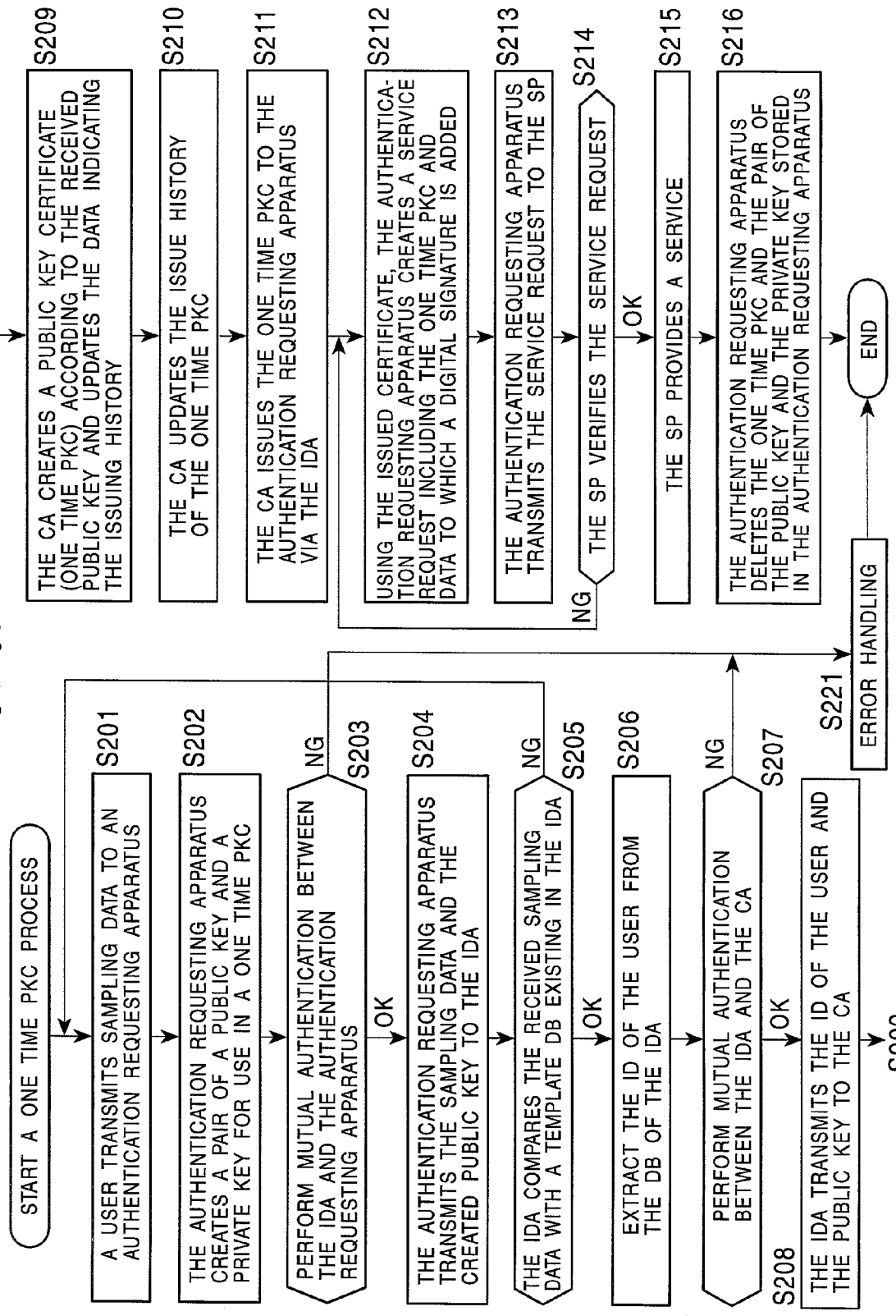

START A ONE TIME PKC PROCESS
A USER TRANSMITS SAMPLING DATA TO AN AUTHENTICATION REQUESTING APPARATUS
S201
THE AUTHENTICATION REQUESTING APPARATUS CREATES A PAIR OF A PUBLIC KEY AND A PRIVATE KEY FOR USE IN A ONE TIME PKC
S202
PERFORM MUTUAL AUTHENTICATION BETWEEN THE IDA AND THE AUTHENTICATION REQUESTING APPARATUS
NG
OK
S203
THE AUTHENTICATION REQUESTING APPARATUS TRANSMITS THE SAMPLING DATA AND THE CREATED PUBLIC KEY TO THE IDA
S204
THE IDA COMPARES THE RECEIVED SAMPLING DATA WITH A TEMPLATE DB EXISTING IN THE IDA
NG
OK
S205
EXTRACT THE ID OF THE USER FROM THE DB OF THE IDA
S206
PERFORM MUTUAL AUTHENTICATION BETWEEN THE IDA AND THE CA
NG
OK
S207
THE IDA TRANSMITS THE ID OF THE USER AND THE PUBLIC KEY TO THE CA
S208
S209
ERROR HANDLING
S221
S208
THE CA CREATES A PUBLIC KEY CERTIFICATE (ONE TIME PKC) ACCORDING TO THE RECEIVED PUBLIC KEY AND UPDATES THE DATA INDICATING THE ISSUING HISTORY
S209
THE CA UPDATES THE ISSUE HISTORY OF THE ONE TIME PKC
S210
THE CA ISSUES THE ONE TIME PKC TO THE AUTHENTICATION REQUESTING APPARATUS VIA THE IDA
S211
USING THE ISSUED CERTIFICATE, THE AUTHENTICATION REQUESTING APPARATUS CREATES A SERVICE REQUEST INCLUDING THE ONE TIME PKC AND DATA TO WHICH A DIGITAL SIGNATURE IS ADDED
S212
THE AUTHENTICATION REQUESTING APPARATUS TRANSMITS THE SERVICE REQUEST TO THE SP
S213
THE SP VERIFIES THE SERVICE REQUEST
NG
OK
S214
THE SP PROVIDES A SERVICE
S215
THE AUTHENTICATION REQUESTING APPARATUS DELETES THE ONE TIME PKC AND THE PAIR OF THE PUBLIC KEY AND THE PRIVATE KEY STORED IN THE AUTHENTICATION REQUESTING APPARATUS
S216
END

FIG. 68

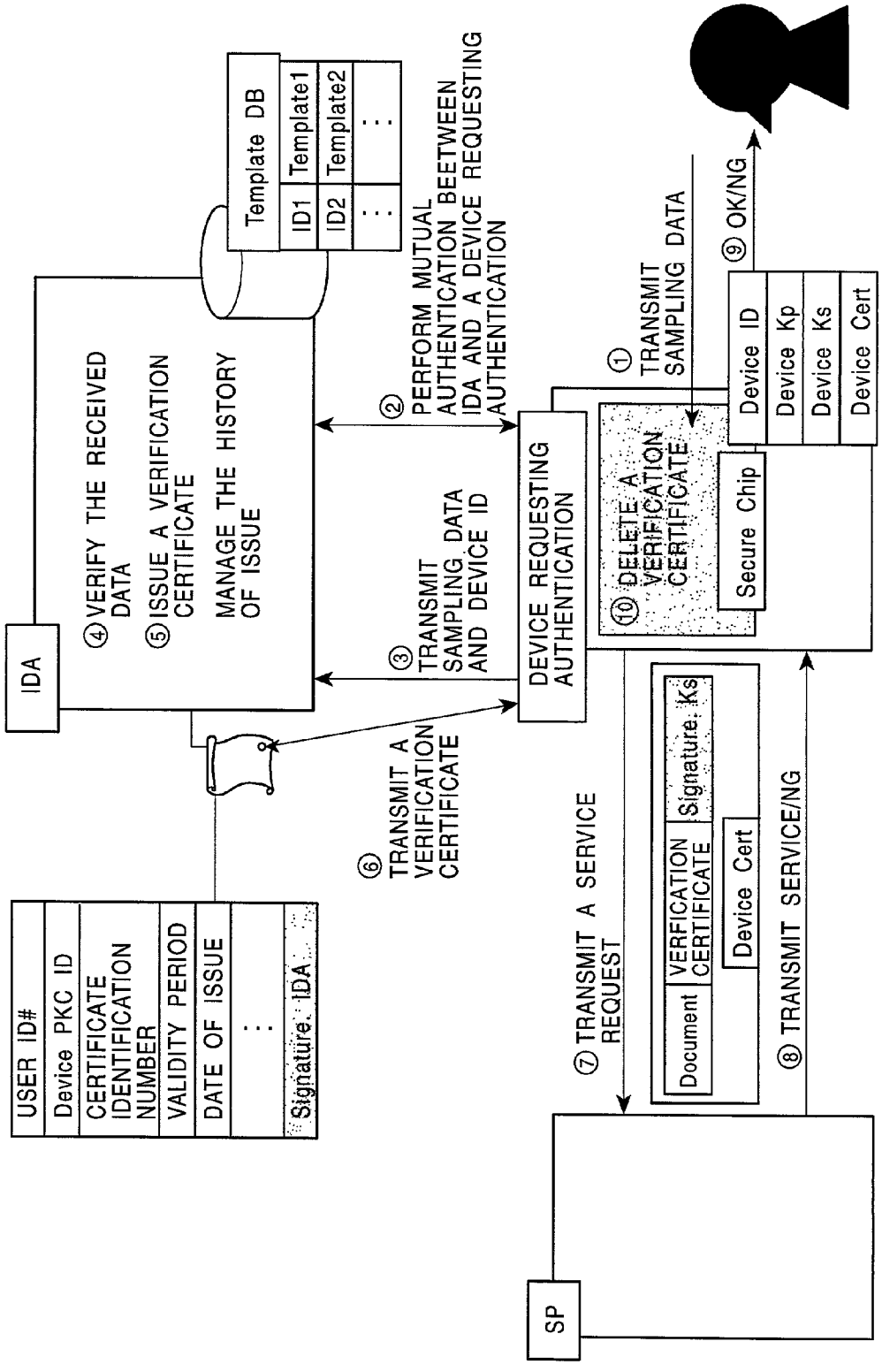

IDA
④ VERIFY THE RECEIVED DATA
⑤ ISSUE A VERIFICATION CERTIFICATE
MANAGE THE HISTORY OF ISSUE
Template DB
ID1 Template1
ID2 Template2
② PERFORM MUTUAL AUTHENTICATION BEETWEEN IDA AND A DEVICE REQUESTING AUTHENTICATION
③ TRANSMIT SAMPLING DATA AND DEVICE ID
⑥ TRANSMIT A VERIFICATION CERTIFICATE
DEVICE REQUESTING AUTHENTICATION
① TRANSMIT SAMPLING DATA
⑨ OK/NG
⑩ DELETE A VERIFICATION CERTIFICATE
Secure Chip
Device ID
Device Kp
Device Ks
Device Cert
USER ID#
Device PKC ID
CERTIFICATE IDENTIFICATION NUMBER
VALIDITY PERIOD
DATE OF ISSUE
Signature: IDA
⑦ TRANSMIT A SERVICE REQUEST
Document
VERFICATION CERTIFICATE
Signature: Ks
Device Cert
⑧ TRANSMIT SERVICE/NG
SP

FIG. 69

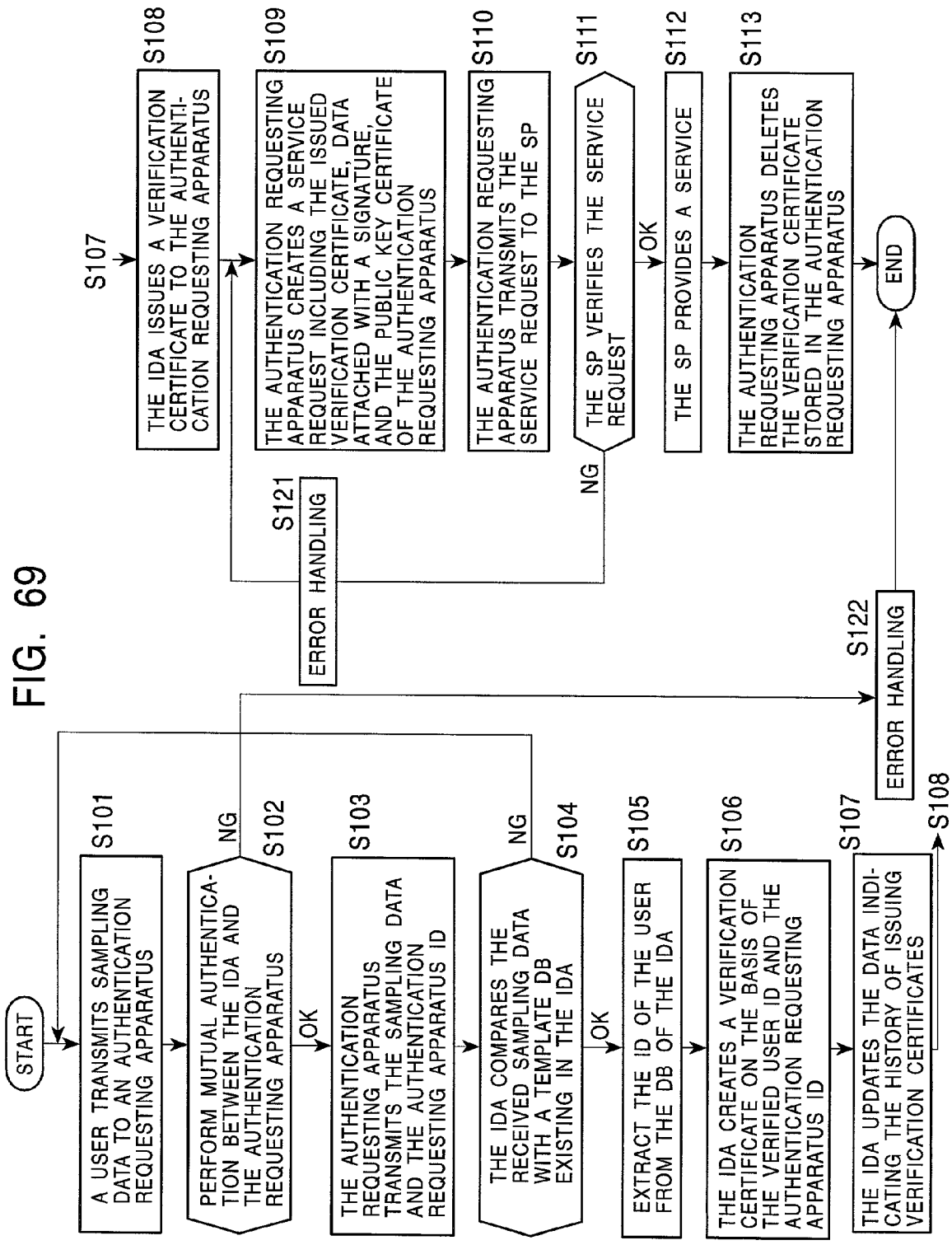

START
A USER TRANSMITS SAMPLING DATA TO AN AUTHENTICATION REQUESTING APPARATUS
S101
PERFORM MUTUAL AUTHENTICATION BETWEEN THE IDA AND THE AUTHENTICATION REQUESTING APPARATUS
S102
NG
OK
THE AUTHENTICATION REQUESTING APPARATUS TRANSMITS THE SAMPLING DATA AND THE AUTHENTICATION REQUESTING APPARATUS ID
S103
THE IDA COMPARES THE RECEIVED SAMPLING DATA WITH A TEMPLATE DB EXISTING IN THE IDA
S104
NG
OK
EXTRACT THE ID OF THE USER FROM THE DB OF THE IDA
S105
THE IDA CREATES A VERIFICATION CERTIFICATE ON THE BASIS OF THE VERIFIED USER ID AND THE AUTHENTICATION REQUESTING APPARATUS ID
S106
THE IDA UPDATES THE DATA INDICATING THE HISTORY OF ISSUING VERIFICATION CERTIFICATES
S107
S108
ERROR HANDLING
S122
END
S107
THE IDA ISSUES A VERIFICATION CERTIFICATE TO THE AUTHENTICATION REQUESTING APPARATUS
S108
THE AUTHENTICATION REQUESTING APPARATUS CREATES A SERVICE REQUEST INCLUDING THE ISSUED VERIFICATION CERTIFICATE, DATA ATTACHED WITH A SIGNATURE, AND THE PUBLIC KEY CERTIFICATE OF THE AUTHENTICATION REQUESTING APPARATUS
S109
THE AUTHENTICATION REQUESTING APPARATUS TRANSMITS THE SERVICE REQUEST TO THE SP
S110
THE SP VERIFIES THE SERVICE REQUEST
S111
NG
OK
THE SP PROVIDES A SERVICE
S112
THE AUTHENTICATION REQUESTING APPARATUS DELETES THE VERIFICATION CERTIFICATE STORED IN THE AUTHENTICATION REQUESTING APPARATUS
S113
ERROR HANDLING
S121

FIG. 70

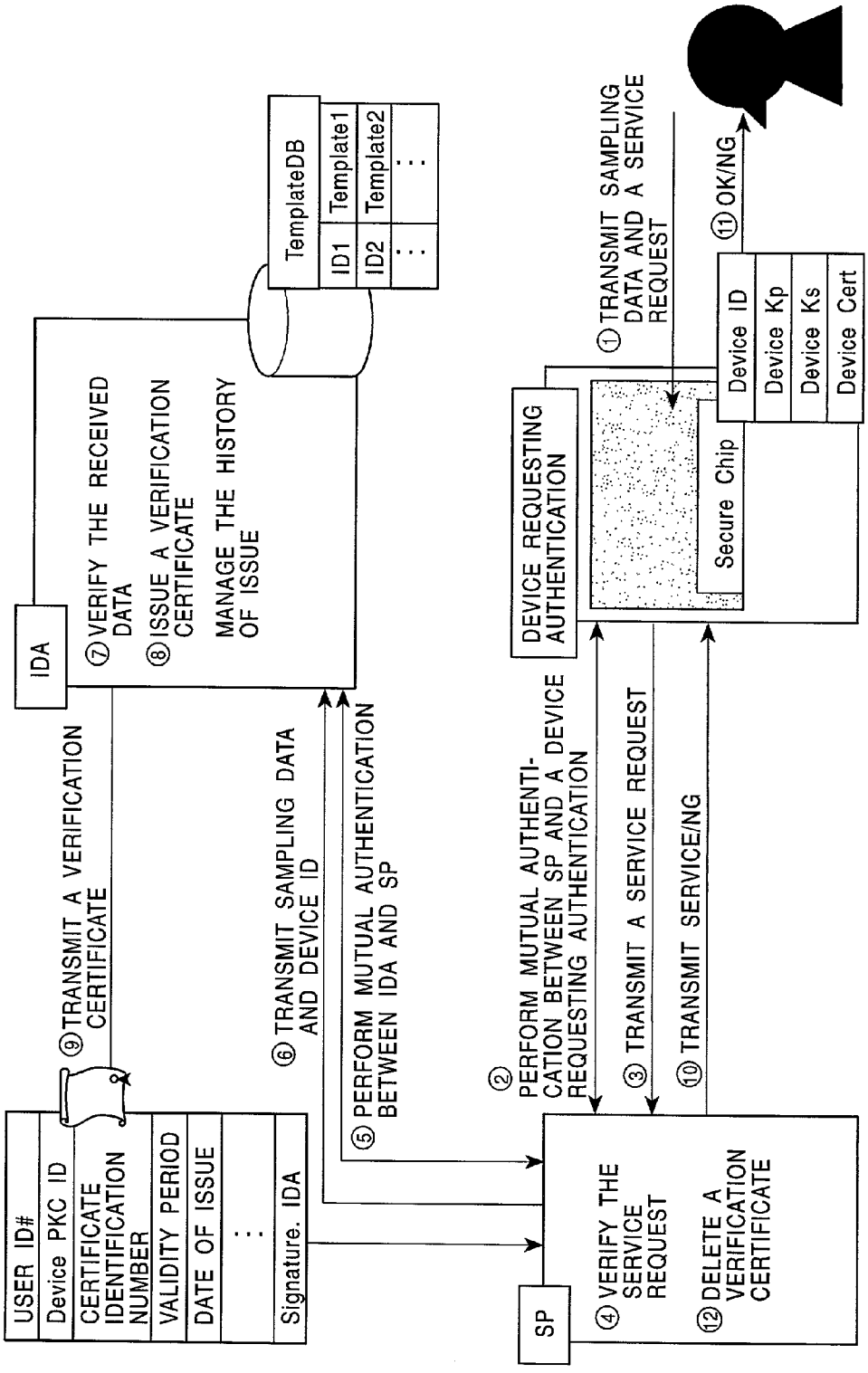

USER ID#
Device PKC ID
CERTIFICATE IDENTIFICATION NUMBER
VALIDITY PERIOD
DATE OF ISSUE
Signature. IDA
⑨TRANSMIT A VERIFICATION CERTIFICATE
IDA
⑦VERIFY THE RECEIVED DATA
⑧ISSUE A VERIFICATION CERTIFICATE
MANAGE THE HISTORY OF ISSUE
TemplateDB
ID1
ID2
Template1
Template2
⑥TRANSMIT SAMPLING DATA AND DEVICE ID
⑤PERFORM MUTUAL AUTHENTICATION BETWEEN IDA AND SP
②PERFORM MUTUAL AUTHENTICATION BETWEEN SP AND A DEVICE REQUESTING AUTHENTICATION
③TRANSMIT A SERVICE REQUEST
⑩TRANSMIT SERVICE/NG
DEVICE REQUESTING AUTHENTICATION
①TRANSMIT SAMPLING DATA AND A SERVICE REQUEST
⑪OK/NG
Secure Chip
Device ID
Device Kp
Device Ks
Device Cert
SP
④VERIFY THE SERVICE REQUEST
⑫DELETE A VERIFICATION CERTIFICATE

FIG. 71

	Item	Description
Indis-pensable Items	Version	Version
	Serial Number	Identification Number
	signature algorithm Identifier algorithm parameters	Signature algorithm Algorithm Parameters
	Issuer	Identification authority name (in the form of a distinguished name)
	Validity notBefore notAfter	Validty period • Start date • Expiration date
	Subject	Subject Name (in a DN form)
	subject IDA Info subject IDA serial Number subject IDA Unique ID	Information about the identification cartificate of the subject • Certificate number of the identification certificate of the subject • Subject unique ID of the identification cerificate of the subject
	subject PKC info subject PKC serial Number subject PKC Unique ID	Information about the public key certificate of the subject • Certificate Number of the public key certificate of the subject • Subject unique ID of the public key certificate of the subject
Indispen-sable	IDA Signature	Signature of IDA

FIG. 72

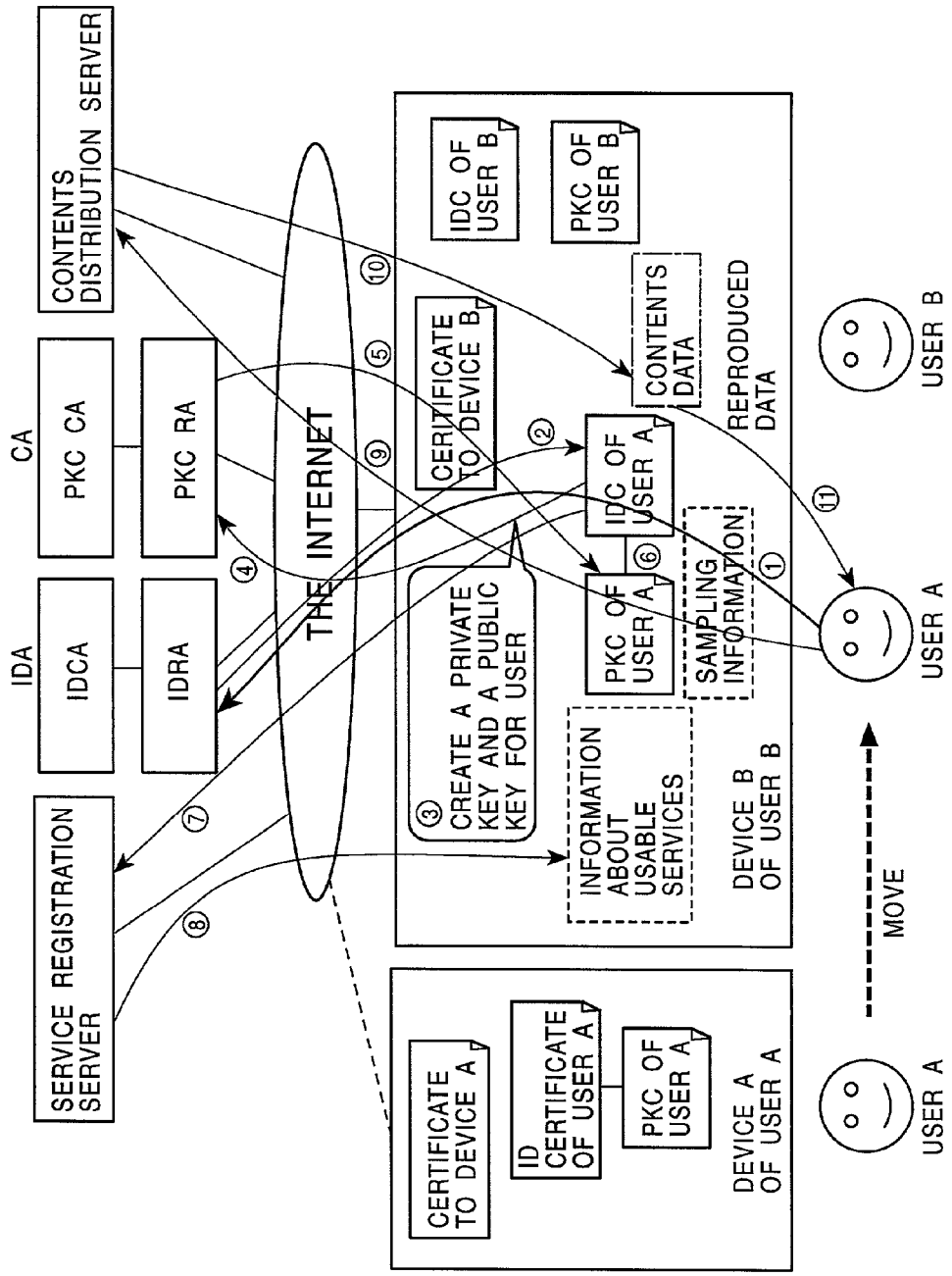

CONTENTS DISTRIBUTION SERVER
CA
PKC CA
PKC RA
IDA
IDCA
IDRA
SERVICE REGISTRATION SERVER
THE INTERNET
IDC OF USER B
PKC OF USER B
CERTIFICATE TO DEVICE B
CONTENTS DATA
REPRODUCED DATA
IDC OF USER A
PKC OF USER A
SAMPLING INFORMATION
③ CREATE A PRIVATE KEY AND A PUBLIC KEY FOR USER
INFORMATION ABOUT USABLE SERVICES
DEVICE B OF USER B
CERTIFICATE TO DEVICE A
ID CERTIFICATE OF USER A
PKC OF USER A
DEVICE A OF USER A
USER A
USER B
MOVE
USER A
USER B

FIG. 73

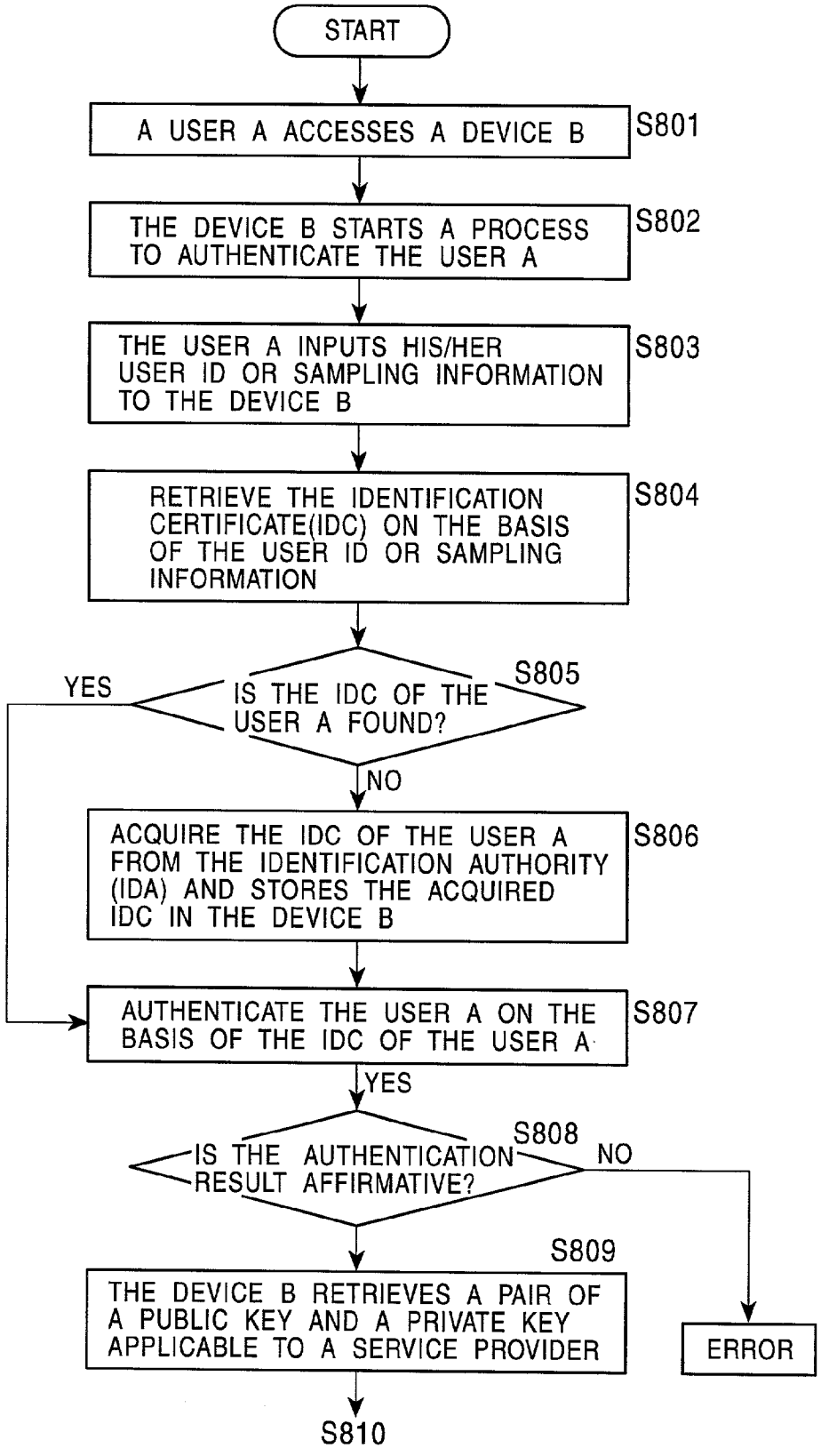

START
A USER A ACCESSES A DEVICE B
S801
THE DEVICE B STARTS A PROCESS TO AUTHENTICATE THE USER A
S802
THE USER A INPUTS HIS/HER USER ID OR SAMPLING INFORMATION TO THE DEVICE B
S803
RETRIEVE THE IDENTIFICATION CERTIFICATE(IDC) ON THE BASIS OF THE USER ID OR SAMPLING INFORMATION
S804
IS THE IDC OF THE USER A FOUND?
S805
YES
NO
ACQUIRE THE IDC OF THE USER A FROM THE IDENTIFICATION AUTHORITY (IDA) AND STORES THE ACQUIRED IDC IN THE DEVICE B
S806
AUTHENTICATE THE USER A ON THE BASIS OF THE IDC OF THE USER A
S807
YES
IS THE AUTHENTICATION RESULT AFFIRMATIVE?
S808
NO
S809
THE DEVICE B RETRIEVES A PAIR OF A PUBLIC KEY AND A PRIVATE KEY APPLICABLE TO A SERVICE PROVIDER
ERROR
S810

FIG. 74

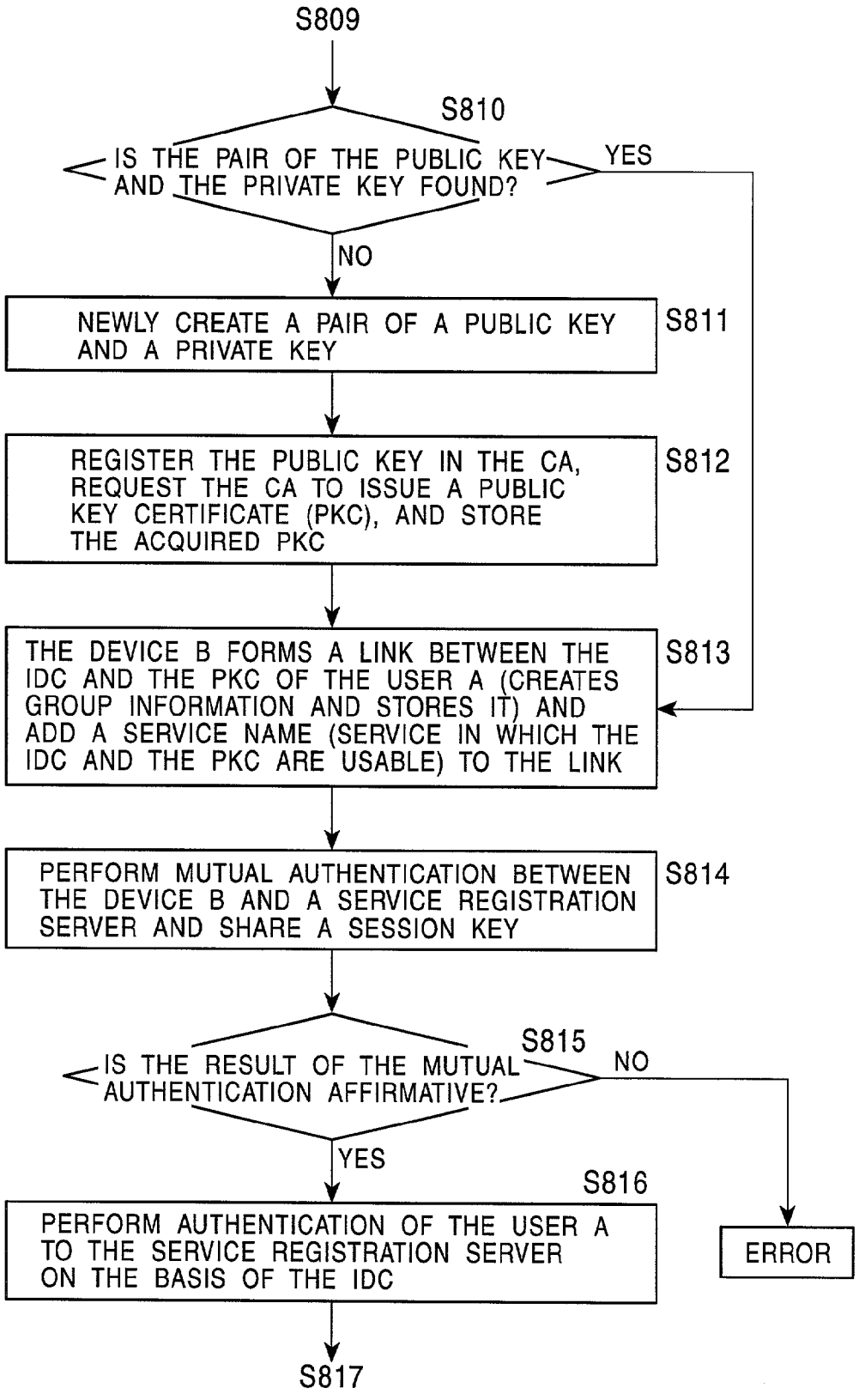

S809
S810
IS THE PAIR OF THE PUBLIC KEY AND THE PRIVATE KEY FOUND?
YES
NO
NEWLY CREATE A PAIR OF A PUBLIC KEY AND A PRIVATE KEY
S811
REGISTER THE PUBLIC KEY IN THE CA, REQUEST THE CA TO ISSUE A PUBLIC KEY CERTIFICATE (PKC), AND STORE THE ACQUIRED PKC
S812
THE DEVICE B FORMS A LINK BETWEEN THE IDC AND THE PKC OF THE USER A (CREATES GROUP INFORMATION AND STORES IT) AND ADD A SERVICE NAME (SERVICE IN WHICH THE IDC AND THE PKC ARE USABLE) TO THE LINK
S813
PERFORM MUTUAL AUTHENTICATION BETWEEN THE DEVICE B AND A SERVICE REGISTRATION SERVER AND SHARE A SESSION KEY
S814
S815
IS THE RESULT OF THE MUTUAL AUTHENTICATION AFFIRMATIVE?
NO
YES
S816
PERFORM AUTHENTICATION OF THE USER A TO THE SERVICE REGISTRATION SERVER ON THE BASIS OF THE IDC
ERROR
S817

FIG. 75

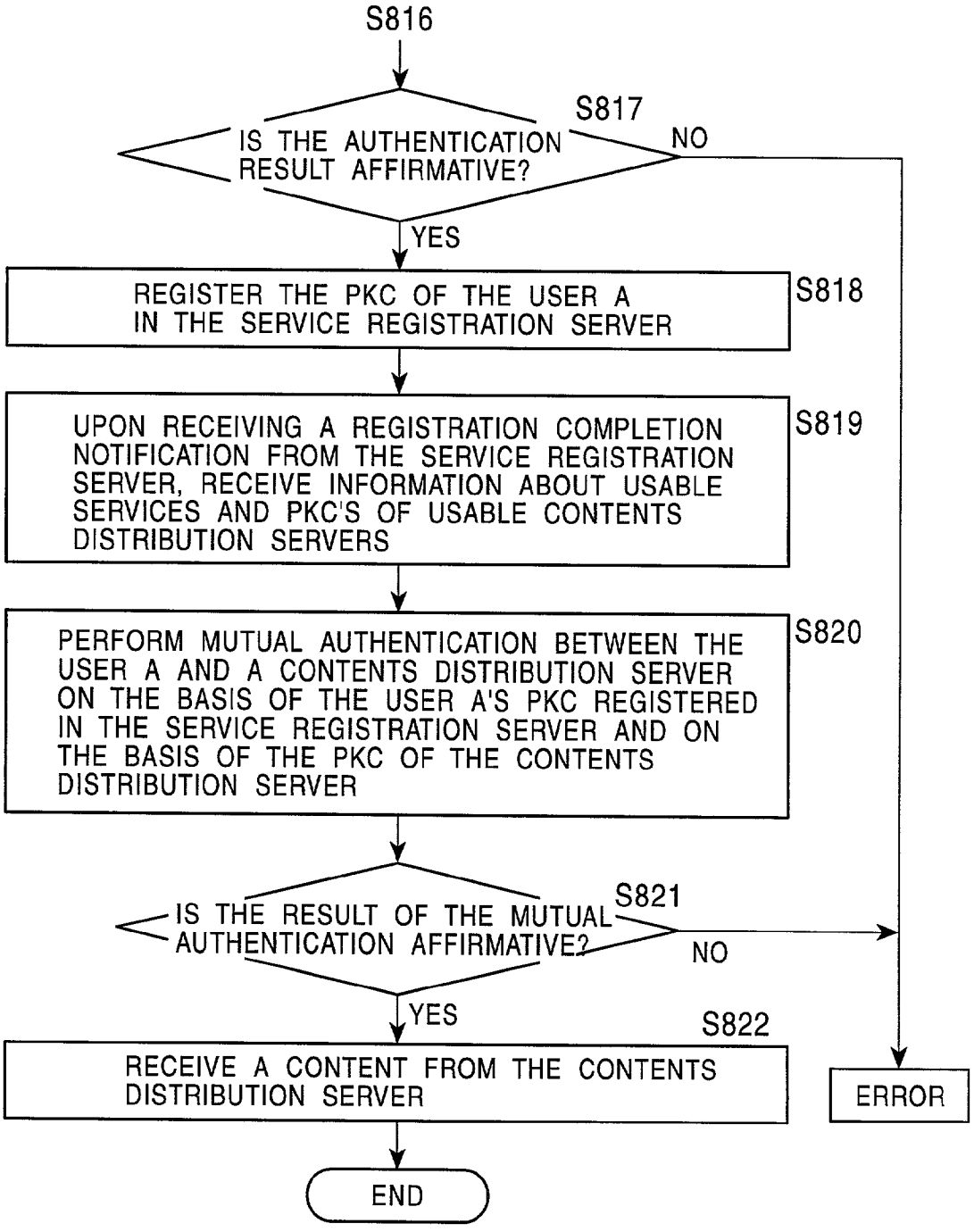

S816
S817
IS THE AUTHENTICATION RESULT AFFIRMATIVE?
NO
YES
REGISTER THE PKC OF THE USER A IN THE SERVICE REGISTRATION SERVER
S818
UPON RECEIVING A REGISTRATION COMPLETION NOTIFICATION FROM THE SERVICE REGISTRATION SERVER, RECEIVE INFORMATION ABOUT USABLE SERVICES AND PKC'S OF USABLE CONTENTS DISTRIBUTION SERVERS
S819
PERFORM MUTUAL AUTHENTICATION BETWEEN THE USER A AND A CONTENTS DISTRIBUTION SERVER ON THE BASIS OF THE USER A'S PKC REGISTERED IN THE SERVICE REGISTRATION SERVER AND ON THE BASIS OF THE PKC OF THE CONTENTS DISTRIBUTION SERVER
S820
IS THE RESULT OF THE MUTUAL AUTHENTICATION AFFIRMATIVE?
S821
NO
YES
RECEIVE A CONTENT FROM THE CONTENTS DISTRIBUTION SERVER
S822
ERROR
END

FIG. 76

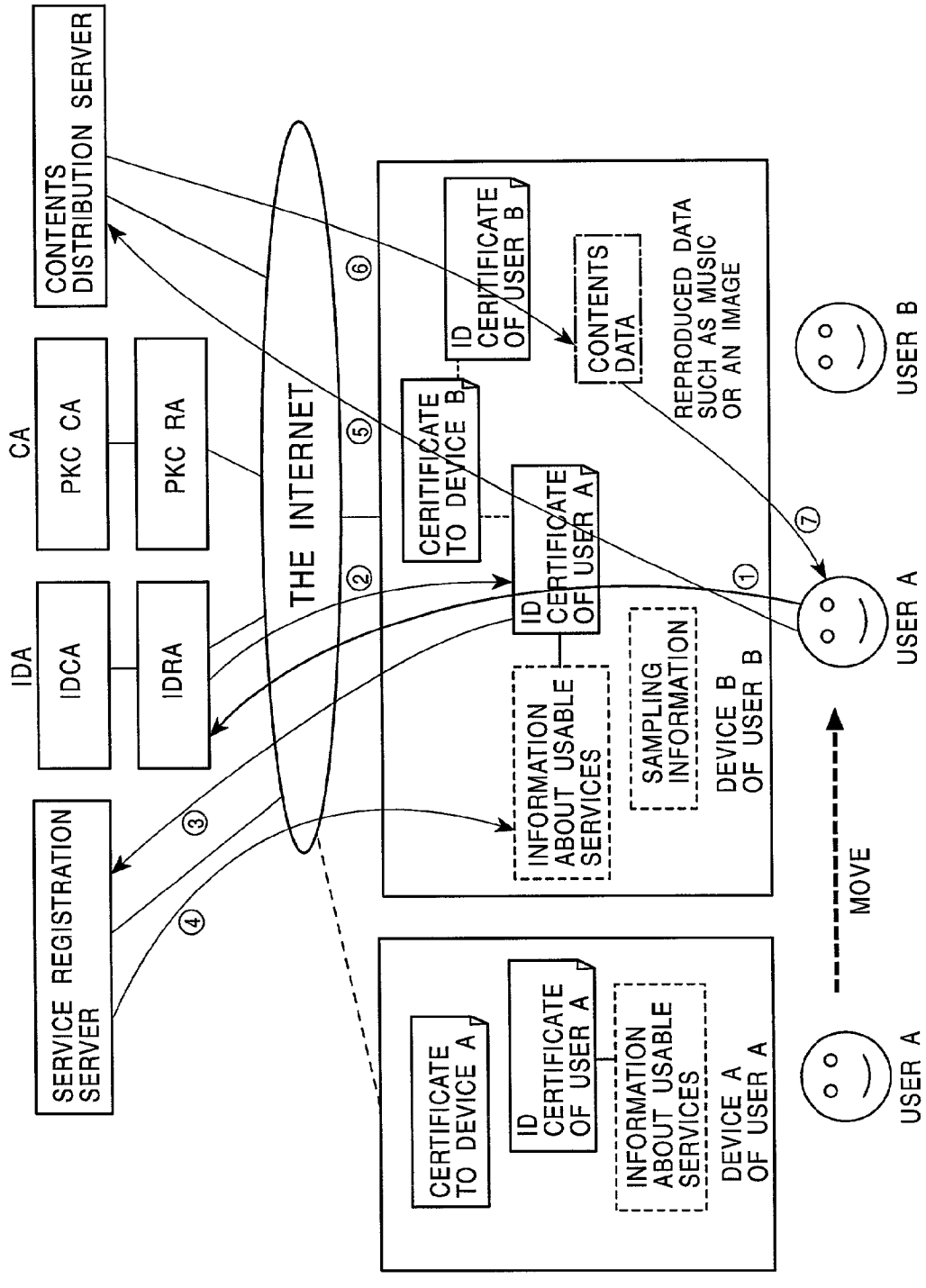

CONTENTS DISTRIBUTION SERVER
CA
PKC CA
PKC RA
IDA
IDCA
IDRA
SERVICE REGISTRATION SERVER
THE INTERNET
①
②
③
④
⑤
⑥
⑦
ID CERTIFICATE OF USER B
CONTENTS DATA
REPRODUCED DATA SUCH AS MUSIC OR AN IMAGE
CERITIFICATE TO DEVICE B
ID CERTIFICATE OF USER A
INFORMATION ABOUT USABLE SERVICES
SAMPLING INFORMATION
DEVICE B OF USER B
USER B
USER A
MOVE
CERTIFICATE TO DEVICE A
ID CERTIFICATE OF USER A
INFORMATION ABOUT USABLE SERVICES
DEVICE A OF USER A
USER A

FIG. 77

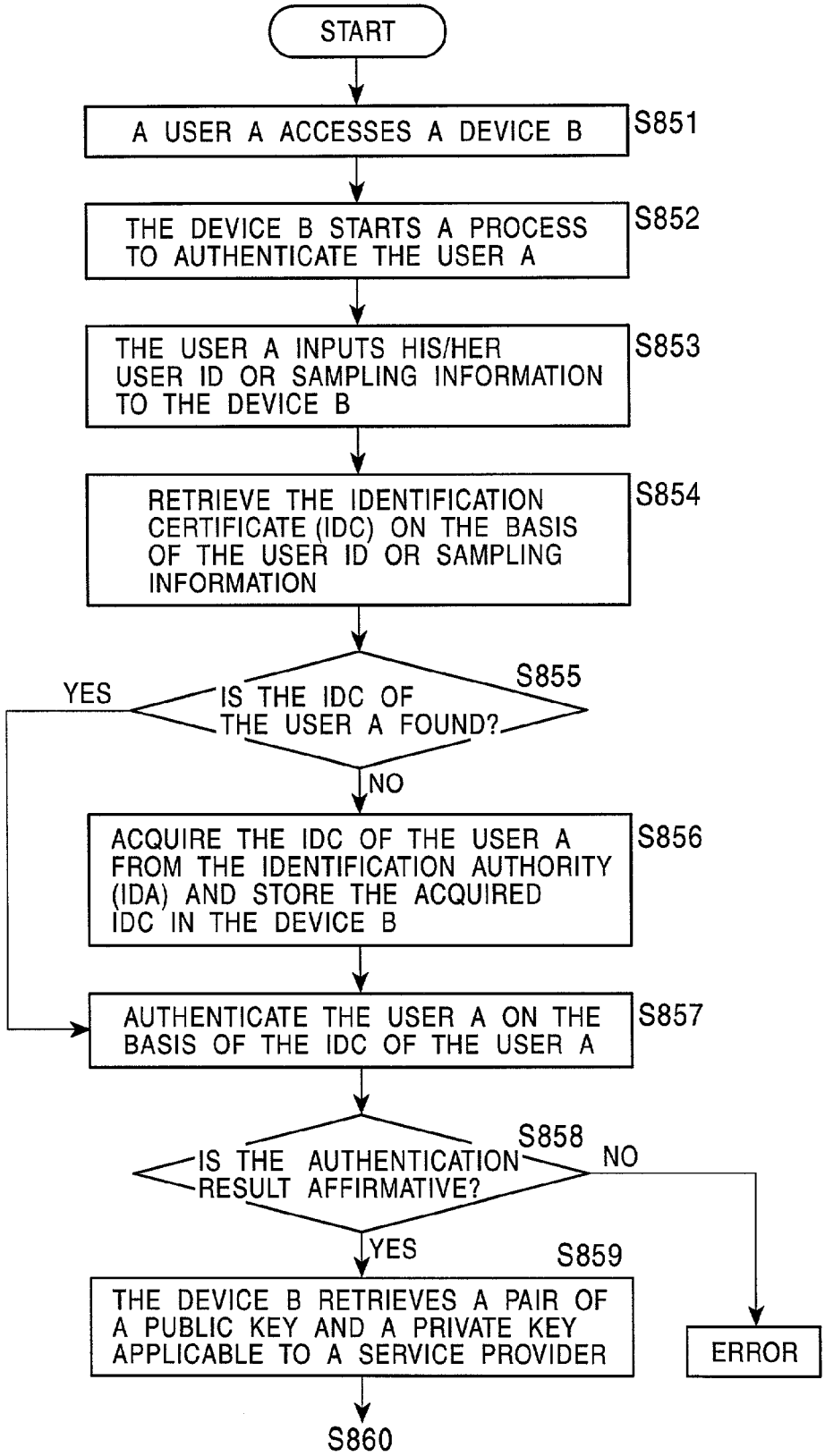

START
A USER A ACCESSES A DEVICE B
S851
THE DEVICE B STARTS A PROCESS TO AUTHENTICATE THE USER A
S852
THE USER A INPUTS HIS/HER USER ID OR SAMPLING INFORMATION TO THE DEVICE B
S853
RETRIEVE THE IDENTIFICATION CERTIFICATE (IDC) ON THE BASIS OF THE USER ID OR SAMPLING INFORMATION
S854
IS THE IDC OF THE USER A FOUND?
S855
YES
NO
ACQUIRE THE IDC OF THE USER A FROM THE IDENTIFICATION AUTHORITY (IDA) AND STORE THE ACQUIRED IDC IN THE DEVICE B
S856
AUTHENTICATE THE USER A ON THE BASIS OF THE IDC OF THE USER A
S857
IS THE AUTHENTICATION RESULT AFFIRMATIVE?
S858
NO
YES
THE DEVICE B RETRIEVES A PAIR OF A PUBLIC KEY AND A PRIVATE KEY APPLICABLE TO A SERVICE PROVIDER
S859
ERROR
S860

FIG. 78

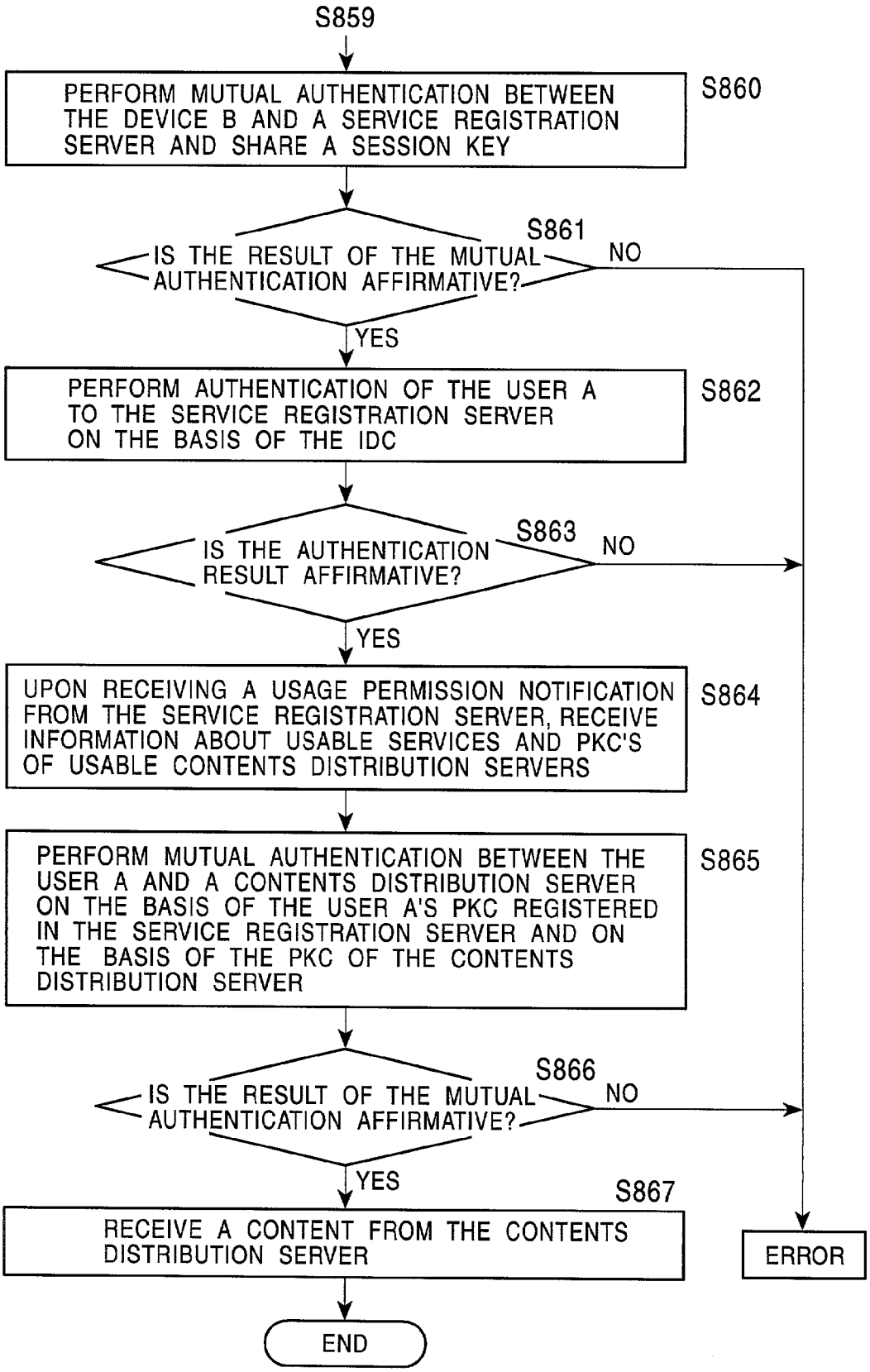

S859
PERFORM MUTUAL AUTHENTICATION BETWEEN THE DEVICE B AND A SERVICE REGISTRATION SERVER AND SHARE A SESSION KEY
S860
IS THE RESULT OF THE MUTUAL AUTHENTICATION AFFIRMATIVE?
S861
NO
YES
PERFORM AUTHENTICATION OF THE USER A TO THE SERVICE REGISTRATION SERVER ON THE BASIS OF THE IDC
S862
IS THE AUTHENTICATION RESULT AFFIRMATIVE?
S863
NO
YES
UPON RECEIVING A USAGE PERMISSION NOTIFICATION FROM THE SERVICE REGISTRATION SERVER, RECEIVE INFORMATION ABOUT USABLE SERVICES AND PKC'S OF USABLE CONTENTS DISTRIBUTION SERVERS
S864
PERFORM MUTUAL AUTHENTICATION BETWEEN THE USER A AND A CONTENTS DISTRIBUTION SERVER ON THE BASIS OF THE USER A'S PKC REGISTERED IN THE SERVICE REGISTRATION SERVER AND ON THE BASIS OF THE PKC OF THE CONTENTS DISTRIBUTION SERVER
S865
IS THE RESULT OF THE MUTUAL AUTHENTICATION AFFIRMATIVE?
S866
NO
YES
RECEIVE A CONTENT FROM THE CONTENTS DISTRIBUTION SERVER
S867
ERROR
END

FIG. 79

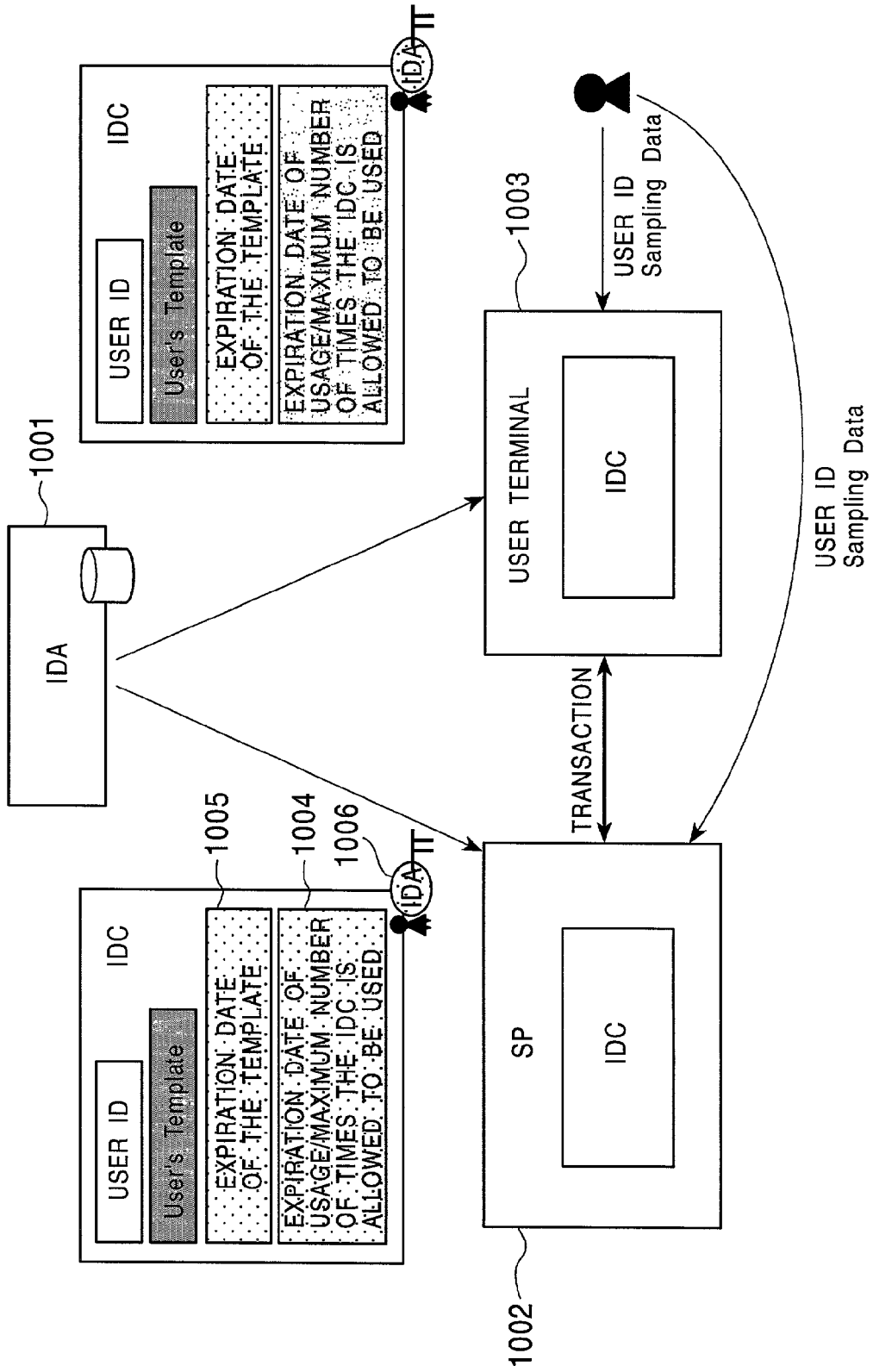

IDC
USER ID
User's Template
EXPIRATION DATE OF THE TEMPLATE
EXPIRATION DATE OF USAGE/MAXIMUM NUMBER OF TIMES THE IDC IS ALLOWED TO BE USED
IDA
1001
IDA
1005
1004
1006
USER TERMINAL
1003
USER ID Sampling Data
TRANSACTION
SP
1002
USER ID Sampling Data

FIG. 80A

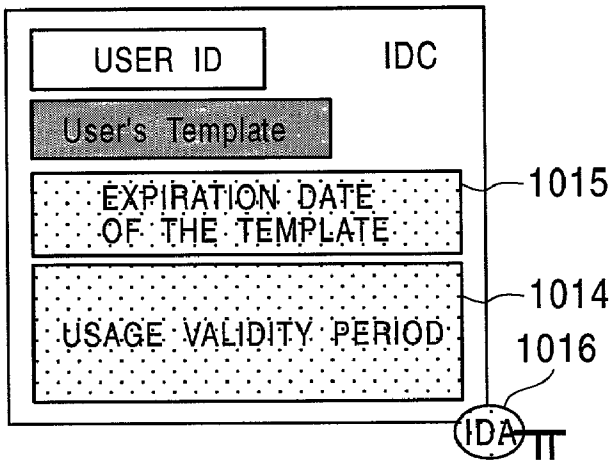


FIG. 80B

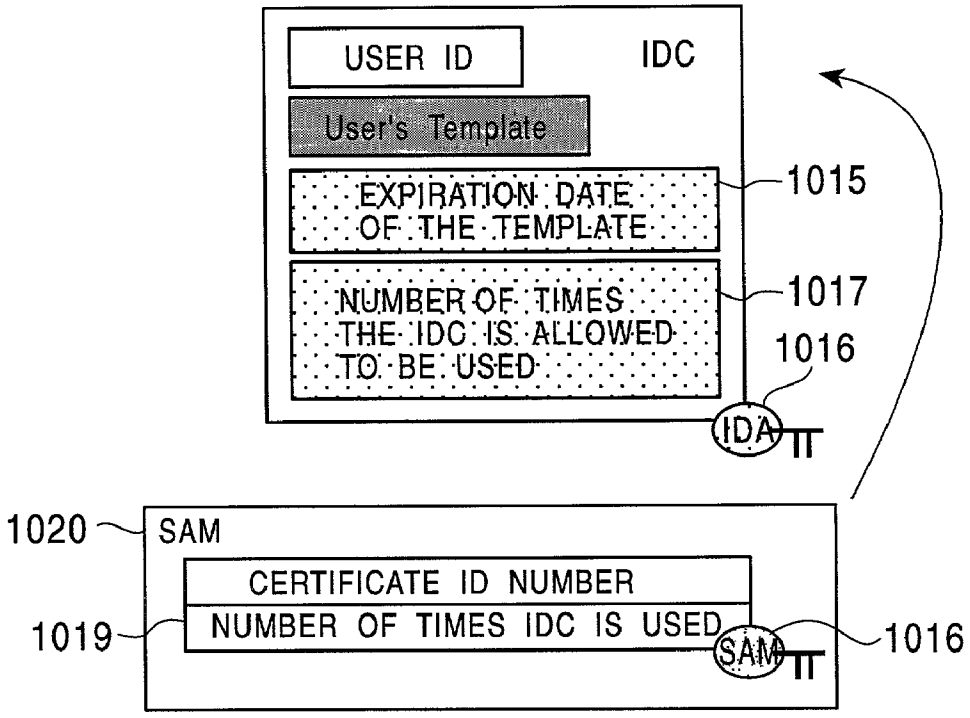


FIG. 81

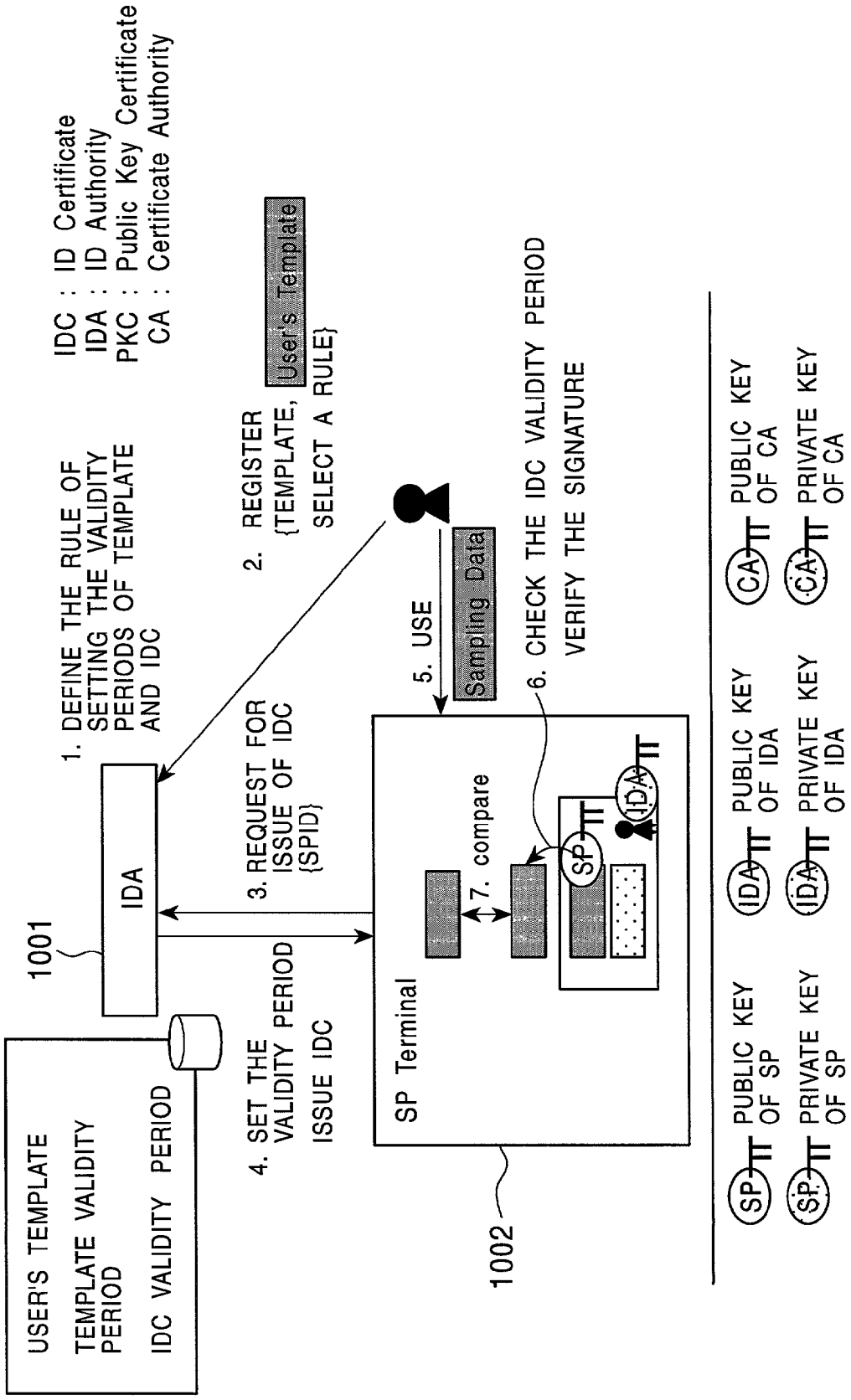

IDC : ID Certificate
IDA : ID Authority
PKC : Public Key Certificate
CA : Certificate Authority
1. DEFINE THE RULE OF SETTING THE VALIDITY PERIODS OF TEMPLATE AND IDC
2. REGISTER {TEMPLATE, SELECT A RULE}
User's Template
3. REQUEST FOR ISSUE OF IDC {SPID}
4. SET THE VALIDITY PERIOD
ISSUE IDC
5. USE
Sampling Data
6. CHECK THE IDC VALIDITY PERIOD
VERIFY THE SIGNATURE
7. compare
1001
IDA
USER'S TEMPLATE
TEMPLATE VALIDITY PERIOD
IDC VALIDITY PERIOD
SP Terminal
1002
SP
IDA
PUBLIC KEY OF SP
PRIVATE KEY OF SP
PUBLIC KEY OF IDA
PRIVATE KEY OF IDA
PUBLIC KEY OF CA
PRIVATE KEY OF CA

FIG. 82

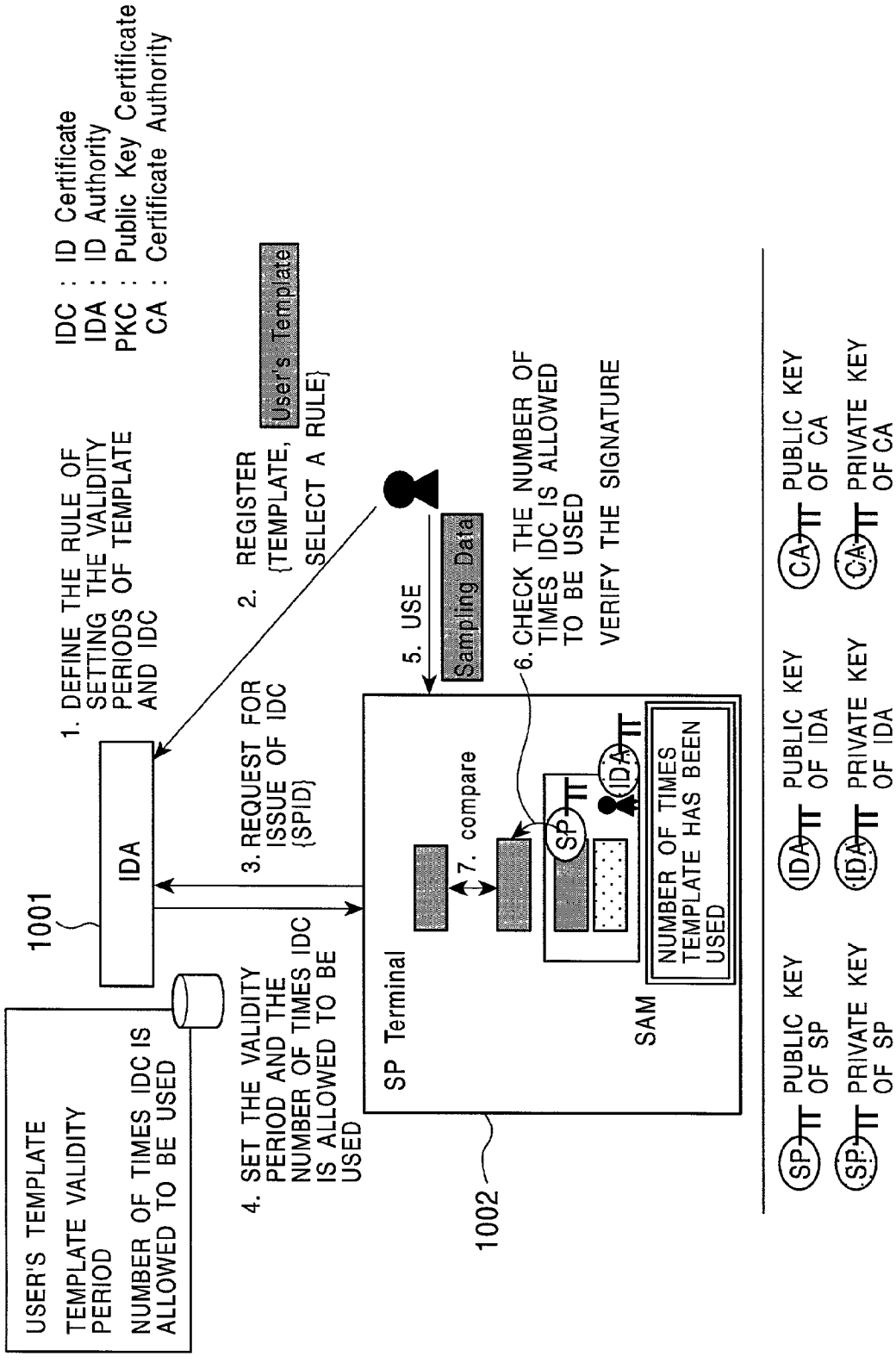

IDC : ID Certificate
IDA : ID Authority
PKC : Public Key Certificate
CA : Certificate Authority
1. DEFINE THE RULE OF SETTING THE VALIDITY PERIODS OF TEMPLATE AND IDC
2. REGISTER {TEMPLATE, SELECT A RULE}
User's Template
3. REQUEST FOR ISSUE OF IDC {SPID}
4. SET THE VALIDITY PERIOD AND THE NUMBER OF TIMES IDC IS ALLOWED TO BE USED
5. USE
Sampling Data
6. CHECK THE NUMBER OF TIMES IDC IS ALLOWED TO BE USED
VERIFY THE SIGNATURE
7. compare
1001
1002
IDA
USER'S TEMPLATE
TEMPLATE VALIDITY PERIOD
NUMBER OF TIMES IDC IS ALLOWED TO BE USED
SP Terminal
SAM
NUMBER OF TIMES TEMPLATE HAS BEEN USED
SP
IDA
CA
PUBLIC KEY OF SP
PRIVATE KEY OF SP
PUBLIC KEY OF IDA
PRIVATE KEY OF IDA
PUBLIC KEY OF CA
PRIVATE KEY OF CA

FIG. 83

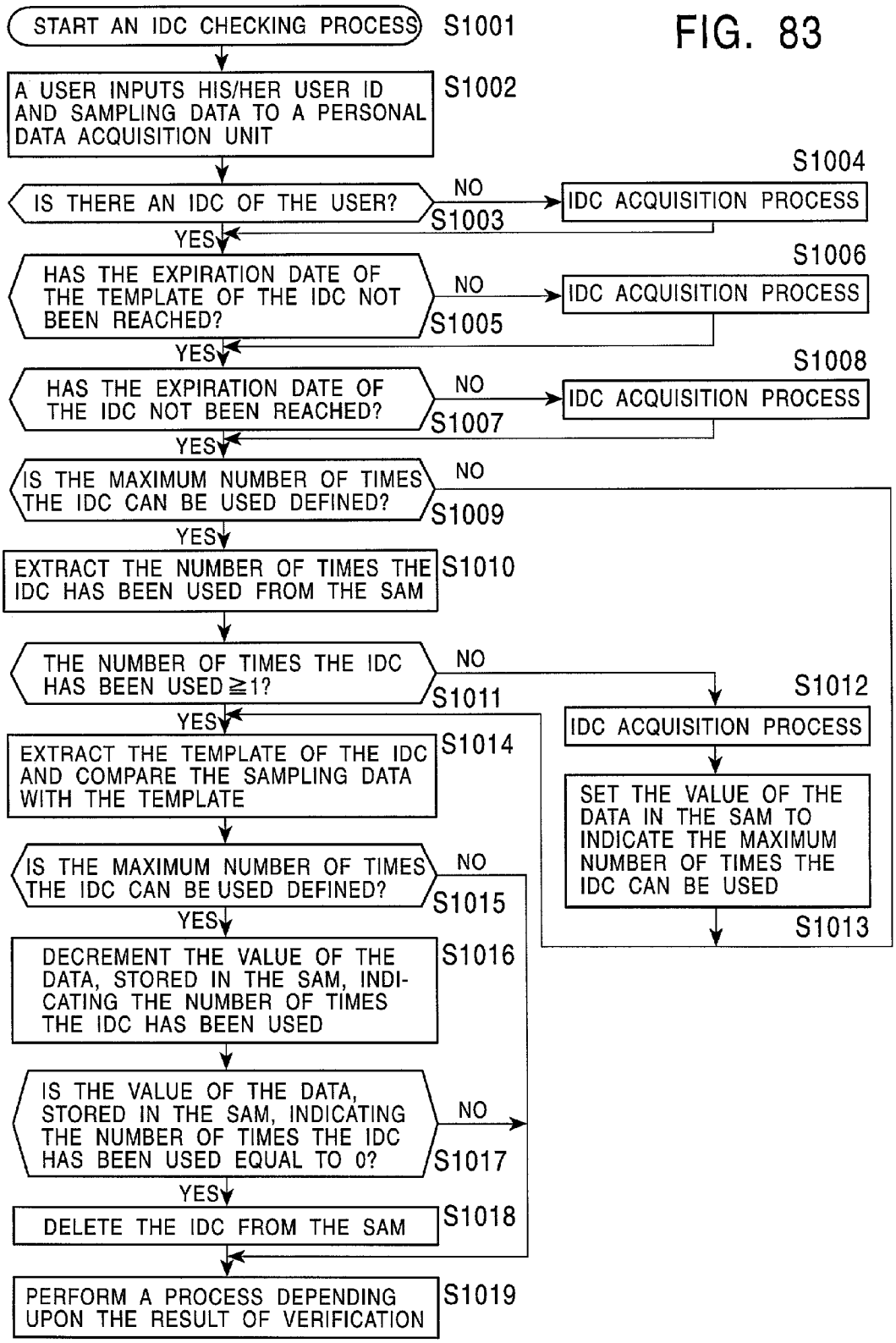

START AN IDC CHECKING PROCESS
S1001
A USER INPUTS HIS/HER USER ID AND SAMPLING DATA TO A PERSONAL DATA ACQUISITION UNIT
S1002
IS THERE AN IDC OF THE USER?
NO
S1003
IDC ACQUISITION PROCESS
S1004
YES
HAS THE EXPIRATION DATE OF THE TEMPLATE OF THE IDC NOT BEEN REACHED?
NO
S1005
IDC ACQUISITION PROCESS
S1006
YES
HAS THE EXPIRATION DATE OF THE IDC NOT BEEN REACHED?
NO
S1007
IDC ACQUISITION PROCESS
S1008
YES
IS THE MAXIMUM NUMBER OF TIMES THE IDC CAN BE USED DEFINED?
NO
S1009
YES
EXTRACT THE NUMBER OF TIMES THE IDC HAS BEEN USED FROM THE SAM
S1010
THE NUMBER OF TIMES THE IDC HAS BEEN USED ≧1?
NO
S1011
IDC ACQUISITION PROCESS
S1012
SET THE VALUE OF THE DATA IN THE SAM TO INDICATE THE MAXIMUM NUMBER OF TIMES THE IDC CAN BE USED
S1013
YES
EXTRACT THE TEMPLATE OF THE IDC AND COMPARE THE SAMPLING DATA WITH THE TEMPLATE
S1014
IS THE MAXIMUM NUMBER OF TIMES THE IDC CAN BE USED DEFINED?
NO
S1015
YES
DECREMENT THE VALUE OF THE DATA, STORED IN THE SAM, INDICATING THE NUMBER OF TIMES THE IDC HAS BEEN USED
S1016
IS THE VALUE OF THE DATA, STORED IN THE SAM, INDICATING THE NUMBER OF TIMES THE IDC HAS BEEN USED EQUAL TO 0?
NO
S1017
YES
DELETE THE IDC FROM THE SAM
S1018
PERFORM A PROCESS DEPENDING UPON THE RESULT OF VERIFICATION
S1019

FIG. 84

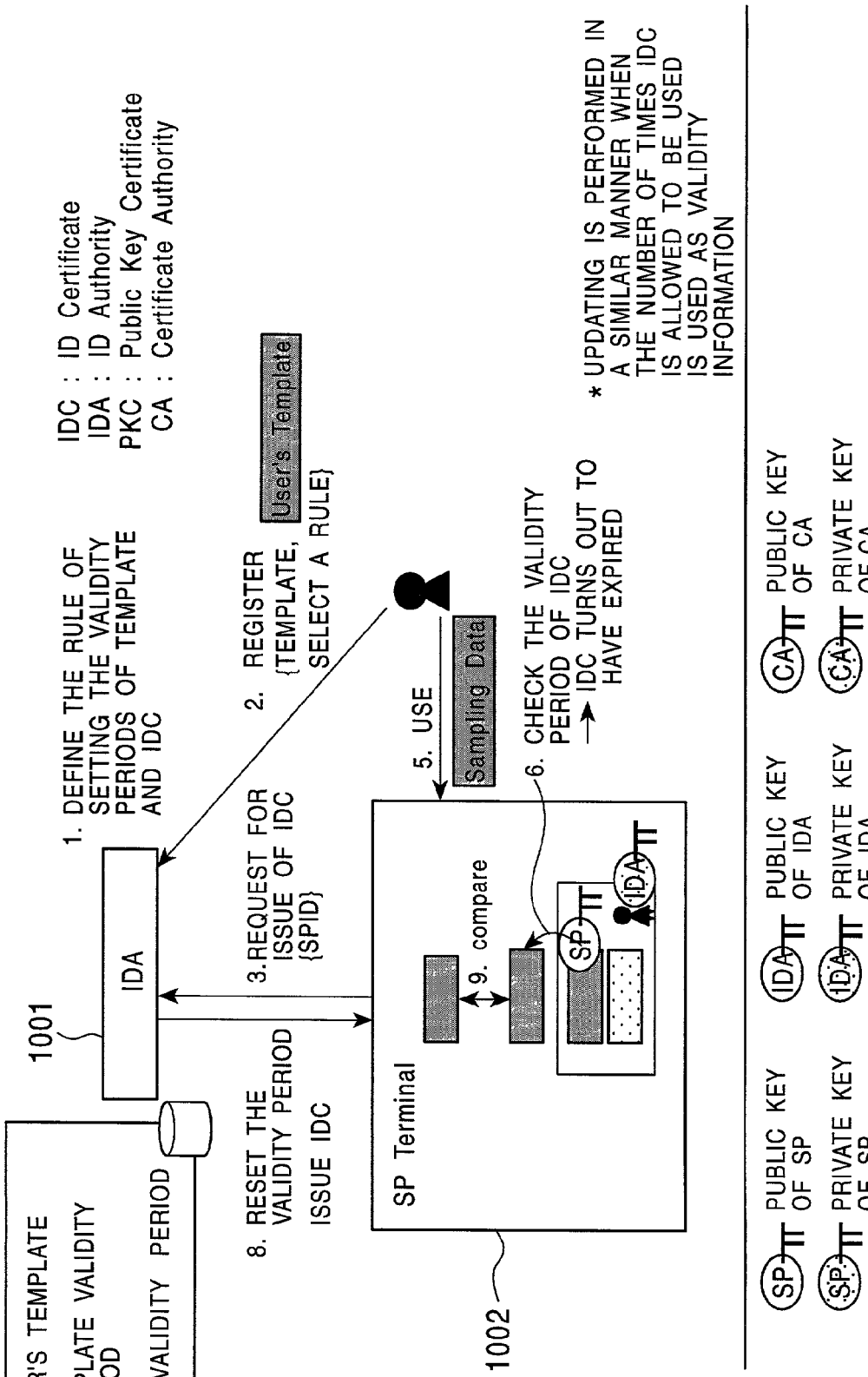

IDC : ID Certificate
IDA : ID Authority
PKC : Public Key Certificate
CA : Certificate Authority
1. DEFINE THE RULE OF SETTING THE VALIDITY PERIODS OF TEMPLATE AND IDC
2. REGISTER {TEMPLATE, SELECT A RULE}
User's Template
3.REQUEST FOR ISSUE OF IDC {SPID}
5. USE
Sampling Data
6. CHECK THE VALIDITY PERIOD OF IDC
IDC TURNS OUT TO HAVE EXPIRED
* UPDATING IS PERFORMED IN A SIMILAR MANNER WHEN THE NUMBER OF TIMES IDC IS ALLOWED TO BE USED IS USED AS VALIDITY INFORMATION
1001
IDA
USER'S TEMPLATE
TEMPLATE VALIDITY PERIOD
IDC VALIDITY PERIOD
8. RESET THE VALIDITY PERIOD
ISSUE IDC
SP Terminal
9. compare
SP
IDA
1002
PUBLIC KEY OF SP
PRIVATE KEY OF SP
PUBLIC KEY OF IDA
PRIVATE KEY OF IDA
PUBLIC KEY OF CA
PRIVATE KEY OF CA

FIG. 85

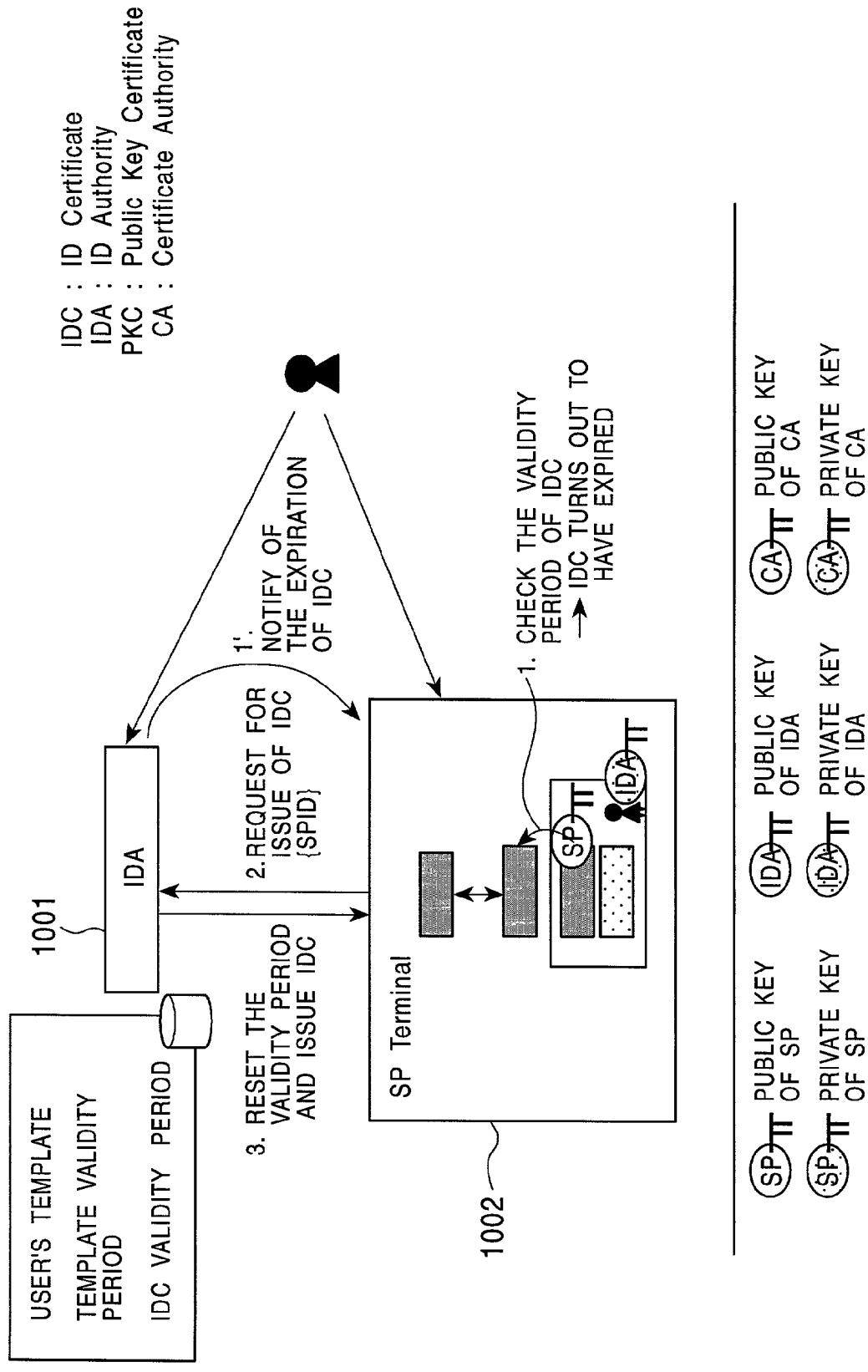

IDC : ID Certificate
IDA : ID Authority
PKC : Public Key Certificate
CA : Certificate Authority
USER'S TEMPLATE
TEMPLATE VALIDITY PERIOD
IDC VALIDITY PERIOD
1001
IDA
1'. NOTIFY OF THE EXPIRATION OF IDC
2. REQUEST FOR ISSUE OF IDC {SPID}
3. RESET THE VALIDITY PERIOD AND ISSUE IDC
1. CHECK THE VALIDITY PERIOD OF IDC
→ IDC TURNS OUT TO HAVE EXPIRED
SP Terminal
1002
SP
IDA
PUBLIC KEY OF SP
PRIVATE KEY OF SP
PUBLIC KEY OF IDA
PRIVATE KEY OF IDA
PUBLIC KEY OF CA
PRIVATE KEY OF CA

FIG. 86

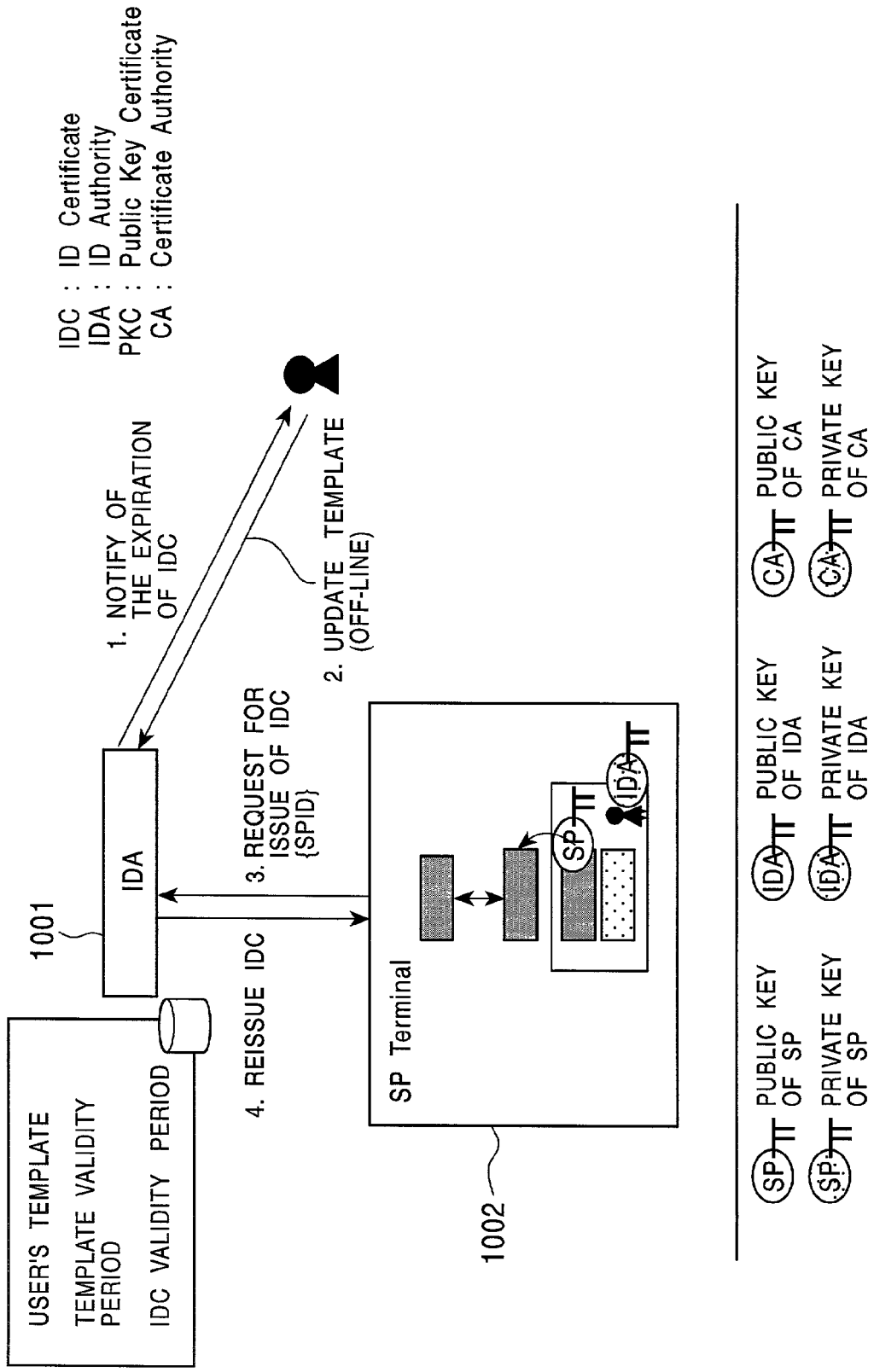
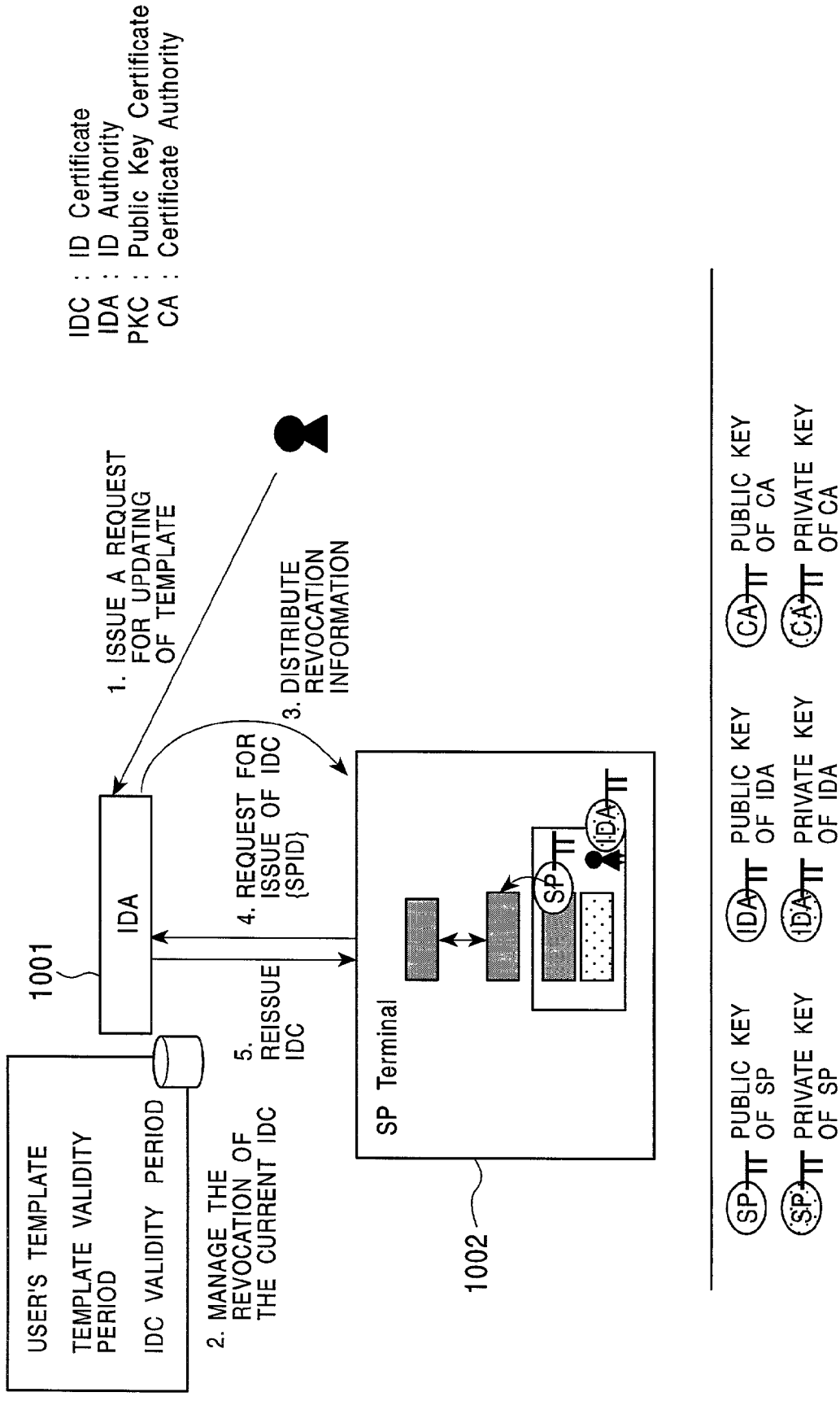

IDC : ID Certificate
IDA : ID Authority
PKC : Public Key Certificate
CA : Certificate Authority
1. NOTIFY OF THE EXPIRATION OF IDC
2. UPDATE TEMPLATE (OFF-LINE)
3. REQUEST FOR ISSUE OF IDC {SPID}
4. REISSUE IDC
1001
IDA
USER'S TEMPLATE
TEMPLATE VALIDITY PERIOD
IDC VALIDITY PERIOD
SP Terminal
1002
SP
IDA
PUBLIC KEY OF SP
PRIVATE KEY OF SP
PUBLIC KEY OF IDA
PRIVATE KEY OF IDA
PUBLIC KEY OF CA
PRIVATE KEY OF CA

FIG. 87


IDC : ID Certificate
IDA : ID Authority
PKC : Public Key Certificate
CA : Certificate Authority
1. ISSUE A REQUEST FOR UPDATING OF TEMPLATE
3. DISTRIBUTE REVOCATION INFORMATION
4. REQUEST FOR ISSUE OF IDC {SPID}
5. REISSUE IDC
2. MANAGE THE REVOCATION OF THE CURRENT IDC
USER'S TEMPLATE
TEMPLATE VALIDITY PERIOD
IDC VALIDITY PERIOD
1001
IDA
SP Terminal
1002
SP
IDA
PUBLIC KEY OF SP
PRIVATE KEY OF SP
PUBLIC KEY OF IDA
PRIVATE KEY OF IDA
PUBLIC KEY OF CA
PRIVATE KEY OF CA

INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING METHOD, AND PROGRAM PROVIDING MEDIUM

BACKGROUND OF THE INVENTION

[0001] 1. Field of the Invention

[0002] The present invention relates to an information processing apparatus, an information processing method, and a program providing medium. More particularly, the present invention relates to an information processing apparatus, an information processing method, and a program providing medium, which can be advantageously employed, in a communication network such as the Internet or in data communication performed via a medium, to identify a person at a receiving end or to authenticate a person who uses an information processing apparatus which receives a service such as receiving of transmitted contents or registration of various services.

[0003] 2. Description of the Related Art

[0004] A data processing apparatus such as a personal computer (PC) is widely used in a company or by a person. In some cases, secret data is stored in such an apparatus. To prevent such secret data from being accessed by an unauthorized user, techniques of preventing information stored in a PC from being leaked have been developed. One known technique for this purpose is to identify a user on the basis of a password input by the user or on the basis of biometric information of the user.

[0005] Now, it is popular to distribute various kinds of software data such as a game program, audio data, image data, and a document generating program (hereinafter, such software data will be referred to as a content) via a network such as the Internet or a storage medium such as a DVD or a CD which can be distributed. In such a situation, it is highly desired to quickly identify a user in a highly reliable fashion in various processes such as distribution of a content or reception of a fee for usage of a content. Furthermore, in the user identification process, it is very important to prevent personal information from being leaked.

[0006] One widely-used user identification method is to compare input data with preassigned data such as a user ID or a password. However, in this method, there is always a possibility that a registered user ID or password is leaked. Once a user ID or password has been leaked, the same user ID or password becomes unusable. One known method to avoid the above problem is to identify a user using biometric information.

[0007] An example of a conventional process of identifying a person using biometric information is described below. A representative example of biometric information for the above purpose is a fingerprint. A person authentication apparatus which reads a fingerprint and verifies it is described below with reference to **FIG. 1**. In **FIG. 1, a** user of a PC **20** registers his/her fingerprint information in a person authentication apparatus **10** including a reading apparatus, and data indicating the fingerprint is stored in a secure memory **14**. The fingerprint information stored therein is called a template. When the user uses data on the personal computer **20**, his/her fingerprint is read and compared with the template by the person authentication apparatus **10** serving as a fingerprint reading apparatus.

[0008] More particularly, reading of fingerprint information of a user is performed by a personal information acquisition unit **11** formed of a CCD camera or the like. After being read, the fingerprint information is subjected to a feature extraction process performed by an information conversion unit **12**, and resultant data is compared, by a comparator **13**, with the template stored in the secure memory **14**.

[0009] The comparator **13** determines whether or not the data is identical to the template on the basis of a threshold value preset in the comparator. If the data and the template match with each other to a degree higher than the threshold value, the comparator **13** outputs an OK signal, while a NG signal is output when the matching degree is lower than the threshold value. The fingerprint information is stored in the form of fingerprint image data, and the data indicating the feature extracted by the information converter **12** is compared with the image data to check the matching degree relative to the threshold value.

[0010] In the case where the comparator **13** determines that the input information and the registered information match with each other, an authentication success message is transmitted to the personal computer **20** via a communication unit **16**, and the user is permitted to access the personal computer **20**. If it is determined that the input data does not match with the registered information, an authentication failure message is transmitted, and accessing to the personal computer **20** is refused. The person authentication apparatus **10** may include fingerprint information templates of a plurality of users (user ID=ID1 to IDn) stored in the secure memory as shown in **FIG. 1**, and a user may be permitted to access the PC if the person authentication apparatus **10** determines that a fingerprint of the user matches with some stored template. This makes it possible for a single person authentication apparatus to deal with a plurality of users.

[0011] However, the above-described person authentication apparatus has the following problems arising from the construction in which templates are stored in a memory of the fingerprint reading/comparing apparatus.

[0012] (a) To use the comparison result, it is required that a template be included in the fingerprint reading/comparing apparatus.

[0013] (b) In the case where a fingerprint is compared at a plurality of different locations, it is required to register, beforehand, the fingerprint in a plurality of fingerprint read/comparison apparatuses.

[0014] (c) Because templates are stored in the fingerprint reading/comparing apparatus, there is a risk that data representing templates may be tampered with or may be read by an unauthorized person.

[0015] (d) When the comparison result is transmitted to a PC or the like, the comparison result can be easily attacked.

[0016] As described above, the conventional person authentication system is coupled in an inseparable fashion to a particular data processing apparatus such as a personal computer which deals with secret information, in which the person authentication system is assumed to authenticate only users who deal with that personal computer, and thus the person authentication system cannot be used to authenticate

a user who uses another device in which no template is stored. Furthermore, because templates are stored in the fingerprint reading/comparing apparatus itself, there is a problem in terms of security and reliability of templates.

[0017] Furthermore, in data transmission in which encrypted data is transmitted via a network or in data distribution via a medium, data is generally encrypted using a public key, and a public key certificate is widely used to guarantee the reliability of the public key. However, although a public key certificate certifies a public key itself, the public key certificate cannot guarantee the relationship between the public key and a person who owns that public key. That is,

[0018] (e) No technique is known to guarantee the relationship between a public key used in transmission of encrypted data or the like and an owner of that public key, and a good enough means for identifying the owner of the public key is not known.

[0019] As described above, the conventional person authentication system has various problems to be solved. In particular, in a recent social situation in which advanced communication systems via networks such as the Internet have become very popular, a large amount of secret information and personal information are frequently dealt with using various communication devices and data processing devices at various locations and at various times. Furthermore, in pay contents distribution systems/services in which contents are distributed to specific users such as registered members, it is required to identify users when contents are distributed or services are provided. Thus, it is highly desired to realize a person authentication system which is usable without having limitations in terms of locations, times, and devices used.

SUMMARY OF THE INVENTION

[0020] Accordingly, it is an object of the present invention to provide an information processing apparatus and an information processing method which allows person authentication to be performed under various circumstances, improves reliability of the person authentication, and realizes safe storage of template information and usage form and further, allows the person authentication to be used in various fields by realizing a usage form related to a public key certificate.

[0021] In particular, it is an object of the present invention to provide an information processing apparatus and an information processing method for executing, by a connection to an external server, a process concerning a service provided by the external server such as a process of receiving contents, wherein person authentication is executed by comparing a template acquired from a person identification certificate storing a template which is person identification data of a user using the information processing apparatus with sampling information input by the user, a connection to the external server such as a contents providing server is executed provided that the authentication is successfully passed, thereby allowing the authentication of the user to be efficiently executed during execution of various services such contents transmission.

[0022] It is another object of the present invention to provide a program providing medium, which executes, on a computer system, information processing for performing, by a connection to an external server, a process concerning a service provided by the external server.

[0023] According to a first aspect of the present invention, there is provided an information processing apparatus for performing, by a connection to an external server, a process concerning a service provided by the external server, wherein the information processing apparatus executes person authentication by comparing a template acquired from a person identification certificate storing a template which is person identification data of a user using the information processing apparatus with sampling information input by the user, and performs connection to the external server provided that the person authentication is successfully passed.

[0024] The information processing apparatus may store a person identification certificate in a memory provided in the information processing apparatus.

[0025] The information processing apparatus may hold link information in which a person identification certificate and a public key certificate applied during a process of establishing a connection to the external server are related to each other, store the person identification certificate and the public key certificate in a memory provided in the information processing apparatus, and extract the public key certificate linked to the person identification certificate on the basis of the link information, provided that personal authentication on the basis of the person identification certificate is successfully passed, and performs mutual authentication between the external server and the information processing apparatus by applying the extracted public key certificate.

[0026] The information processing apparatus may be an apparatus having the function of reproducing contents, the external server may be a contents providing server, and the information processing apparatus may execute person authentication by comparing the template extracted from the person identification certificate with sampling information input by a user, establish a connection to the contents providing server providing that the person authentication is successfully passed, and download the contents.

[0027] In the information processing apparatus, the external server may be one of a user registration server and a service registration server which performs any one of processes of user registration, erasure of user registration, and making a service contract to a service providing entity, and the information processing apparatus may execute person authentication by comparing a template extracted from the person identification certificate with sampling information input by a user, establish a connection to one of the user registration server and the service registration server provided that the person authentication is successfully passed, and transmit necessary data corresponding to any one of the processes of user registration, erasure of user registration, and making a service contract to the user registration server.

[0028] The information processing apparatus may form a link in which a person identification certificate and a public key certificate applied during a process of establishing a connection for data communication with a party is related to each other, and store the link in a storage means thereof.

[0029] The information processing apparatus may download a person identification certificate applied to person authentication from a person identification certificate author-

ity which is an entity for issuing a person identification certificate and store the downloaded person identification certificate in a storage means thereof. In a process of downloading the person identification certificate, the information processing apparatus may perform mutual authentication between the information processing apparatus and the person identification certificate authority, and download the person identification certificate from the person identification certificate authority provided that the mutual authentication is successfully completed.

[0030] The information processing apparatus may download a person identification certificate applied to person authentication from a person identification certificate authority which is an entity for issuing a person identification certificate and store the downloaded person identification certificate. When there is a public key certificate applicable to a process relating to application of the person identification certificate acquired by downloading, the information processing apparatus may update link information in which the person identification certificate and the public key certificate are related to each other, and store the person identification certificate and the public key certificate in a memory provided in the information processing apparatus.

[0031] The information processing apparatus may download a public key certificate from a certificate authority which is an entity for issuing a public key certificate and store the downloaded public key certificate in a storage means thereof. In a process of downloading the public key certificate, the information processing apparatus may perform mutual authentication between the information processing apparatus and the certificate authority, and download the public key certificate from the certificate authority provided that the mutual authentication is successfully completed.

[0032] The information processing apparatus may download a public key certificate from a certificate authority which is an entity for issuing a public key certificate and store the downloaded public key certificate in a storage means thereof. When there is a person identification certificate applicable to a process relating to application of the public key certificate acquired by downloading, the information processing apparatus may update link information in which the person identification certificate and the public key certificate are related to each other, and store the person identification certificate and the public key certificate in a memory provided in the information processing apparatus.

[0033] The information processing apparatus may include an encryption processing unit. In data transmission/reception between the information processing apparatus and the external server, the information processing apparatus may perform mutual authentication between the information processing apparatus and the external server and further, a data transmitting end may add a digital data to the transmitted data and a data receiving end may verify the digital signature.

[0034] In the information processing apparatus, the template may be composed of any one of biometric information of a person such as fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information; non-biometric information such as a seal, a passport, a driver's license, and a card; any combination of two or more of the biometric information and the non-biometric information; and a combination of any of the information and a password.

[0035] According to a second aspect of the present invention, there is provided an information processing method for performing, by a connection to an external server, a process concerning a service provided by the external server, the method including the steps of:

[0036] executing person authentication by comparing a template acquired from a person identification certificate storing a template which is person identification data of a user using an information processing apparatus with sampling information input by the user; and

[0037] performing a connection to the external server provided that the person authentication is successfully passed.

[0038] The information processing method may further include the steps of:

[0039] storing a person identification certificate in a memory provided in the information processing apparatus; and

[0040] executing a process by reading the stored person identification certificate during executing personal authentication.

[0041] In the information processing method, the information processing apparatus may hold link information in which a person identification certificate and a public key certificate applied during a process of establishing a connection to the external server are related to each other and store the person identification certificate and the public key certificate in a memory provided in the information processing apparatus, and the information processing apparatus may extract the public key certificate linked to the person identification certificate on the basis of the link information, provided that personal authentication on the basis of the person identification certificate is successfully passed, and perform mutual authentication between the external server and the information processing apparatus by applying the extracted public key certificate.

[0042] In the information processing method, the information processing apparatus may be an apparatus having the function of reproducing contents, the external server may be a contents providing server, and the information processing apparatus may execute person authentication by comparing the template extracted the person identification certificate with sampling information input by a user, establish a connection to the contents providing server providing that the person authentication is successfully passed, and download the contents.

[0043] In the information processing method, the external server may be one of a user registration server and a service registration server which performs any one of processes of user registration, erasure of user registration, and making a service contract to a service providing entity, and the information processing apparatus may execute person authentication by comparing a template extracted from the person identification certificate with sampling information input by a user, establish a connection to one of the user registration server and the service registration server provided that the person authentication is successfully passed, and transmit necessary data corresponding to any one of the processes of

user registration, erasure of user registration, and making a service contract to the user registration server.

[0044] In the information processing method, the information processing apparatus may form a link in which a person identification certificate and a public key certificate applied during a process of establishing a connection for data communication with a party is related to each other, and store the link in a storage means thereof.

[0045] The information processing method may further include the steps of:

[0046] downloading a person identification certificate applied to person authentication from a person identification certificate authority which is an entity for issuing a person identification certificate to store the downloaded person identification certificate in a storage means thereof;

[0047] performing, in a process of downloading the person identification certificate, mutual authentication between the information processing apparatus and the person identification certificate authority; and

[0048] downloading the person identification certificate from the person identification certificate authority provided that the mutual authentication is successfully completed.

[0049] The information processing method may further include the steps of:

[0050] downloading a person identification certificate applied to person authentication from a person identification certificate authority, which is an entity for issuing a person identification certificate, to store the downloaded person identification certificate; and

[0051] updating, when there is a public key certificate applicable to a process relating to application of the person identification certificate acquired by downloading, link information, in which the person identification certificate and the public key certificate are related to each other, to store the person identification certificate and the public key certificate in a memory provided in the information processing apparatus.

[0052] The information processing apparatus may further include the steps of:

[0053] downloading a public key certificate from a certificate authority, which is an entity for issuing a public key certificate, to store the downloaded public key certificate in a storage means thereof;

[0054] performing, in a process of downloading the public key certificate, mutual authentication between the information processing apparatus and the certificate authority; and

[0055] downloading the public key certificate from the certificate authority provided that the mutual authentication is successfully completed.

[0056] The information processing method may further includes the steps of:

[0057] downloading a public key certificate from a certificate authority, which is an entity for issuing a public key certificate, to store the downloaded public key certificate in a storage means thereof; and

[0058] updating, when there is a person identification certificate applicable to a process relating to application of the public key certificate acquired by downloading, link information, in which the person identification certificate and the public key certificate are related to each other, to store the person identification certificate and the public key certificate in a memory provided in the information processing apparatus.

[0059] In the information processing method, in data transmission/reception between the information processing apparatus and the external server, the information processing apparatus may perform mutual authentication between the information processing apparatus and the external server and further, a data transmitting end may add a digital data to the transmitted data and a data receiving end may verify the digital signature.

[0060] The information processing apparatus and the information processing method according to the present invention allow person authentication to be performed in an easy fashion in various devices by comparing a template serving as person identification data with sampling information input by a user. For example, a service provider (SP) or user device (UD) can execute person authentication by acquiring a template from a person identification certificate (IDC) generated by a third-party agency serving as a person identification certificate authority (IDA). The person identification certificate (IDC) is issued by the person identification certificate authority (IDA), in response to a request from a person, on the basis of a template serving as identification data which is acquired from the person after verifying the identification of the person, and, when the person identification certificate (IDC) is distributed to a service provider (SP) or a user device (UD), the distribution is performed after adding a signature of the IDA thereto, thereby ensuring that the validity of the data is guaranteed and high-reliability person authentication can be performed.

[0061] Furthermore, in the information processing apparatus and the information processing method according to the present invention, in an information processing apparatus for performing, by a connection to an external server, a process concerning a service provided by the external server such as a process of receiving contents, person authentication is executed by comparing a template acquired from a person identification certificate storing a template which is person identification data of a user using the information processing apparatus with sampling information input by a user, a connection to the external server such as a contents providing server is executed provided that the authentication is successfully passed, thereby allowing the authentication of the user to be efficiently executed during execution of various services such contents transmission.

[0062] Furthermore, in the information processing apparatus and the information processing method, link information is held in which a person identification certificate and a public key certificate applied during a process of establishing a connection to the external server are related to each other, and the person identification certificate and the public key certificate are stored in a memory provided in the information processing apparatus. Therefore, it is possible to extract a person identification certificate and a public key certificate required for a series of processes on the basis of the link information, thus realizing efficient information processing.

[0063] According to a third aspect of the present invention, there is provided a program providing medium for

providing a computer program which executes, on a computer system, information processing for performing, by a connection to an external server, a process concerning a service provided by the external server, the computer program including the steps of:

[0064] executing person authentication by comparing a template acquired from a person identification certificate storing a template which is person identification data of a user using an information processing apparatus with sampling information input by the user; and

[0065] performing a connection to the external server provided that the person authentication is successfully passed.

[0066] The program providing medium according to the third aspect of the present invention is used to provide a computer program in a computer-readable format to a computer system capable of executing various program codes. There is no particular limitation in the form of the medium, and various types of media can be used. Specific examples include a storage medium such as a CD, FD, MO, and DVD and a transmission medium such as a network.

[0067] Such a program providing medium defines a cooperative relationship in structure or function between the computer program and the providing medium so that the computer program functions on a computer system. In other words, the program providing medium operates in a cooperative fashion on a computer system when the computer program is installed on the computer system via the program providing medium, thereby achieving functions similar to those which can be achieved according to the other aspects of the present invention.

[0068] Other objects, aspects, and advantages of the present invention will become apparent from the following description of embodiments with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0069] **FIG. 1** is a diagram illustrating a conventional person authentication apparatus which reads and verifies a fingerprint;

[0070] **FIG. 2** is a diagram illustrating encrypted data communication performed, using a public key certificate, by a personal authentication system according to the present invention;

[0071] **FIG. 3** is a diagram illustrating a data format of a public key certificate;

[0072] **FIG. 4** is a diagram illustrating the data format of the public key certificate;

[0073] **FIG. 5** is a diagram illustrating an example of a format of a person identification certificate;

[0074] **FIGS. 6A** to **6C** are diagrams illustrating manners of encrypting a template of a person identification certificate;

[0075] **FIG. 7** is a table illustrating the types of keys used to encrypt a template of a person identification certificate and also illustrating processing manners;

[0076] **FIGS. 8A and 8B** are diagrams illustrating manners of encrypting a template of a person identification certificate;

[0077] **FIG. 9** is a diagram illustrating a processing flow and a data flow in registration of a template and generation of an IDC;

[0078] **FIG. 10** is a diagram illustrating a processing flow and a data flow in a process of deleting a template;

[0079] **FIG. 11** is a diagram illustrating a processing flow and a data flow in a process of changing a template;

[0080] **FIG. 12** is a diagram illustrating a processing flow and a data flow in a process of adding a template;

[0081] **FIG. 13** is a diagram illustrating a processing flow and a data flow in a process of suspending a template;

[0082] **FIG. 14** is a diagram illustrating a processing flow and a data flow in a process of canceling suspension of a template;

[0083] **FIG. 15** is a diagram illustrating a processing flow and a data flow in a process of distributing an IDC;

[0084] **FIG. 16** is a diagram illustrating a processing flow and a data flow in a process of updating an IDC;

[0085] **FIG. 17** is a diagram illustrating a processing flow and a data flow in a process of deleting an IDC;

[0086] **FIG. 18** is a diagram illustrating a processing flow and a data flow in a process of inquiring about an IDC;

[0087] **FIG. 19** is a diagram illustrating examples of configurations of a certificate authority (CA) which issues a public key certificate (PKC), a person identification certificate authority (IDA) which issues a person identification certificate (IDC), and a device which uses a certificate;

[0088] **FIG. 20** is a diagram illustrating examples of configurations of a certificate authority (CA) which issues a public key certificate (PKC), a person identification certificate authority (IDA) which issues a person identification certificate (IDC), and a device which uses a certificate;

[0089] **FIGS. 21A** to **21C** are diagrams illustrating manners of performing verification by a user device, a service provider (SP), or a person identification certificate authority (IDA) in a system;

[0090] **FIG. 22** is a diagram illustrating a system in which verification is performed by a user device;

[0091] **FIG. 23** is a diagram illustrating a system in which verification is performed by a service provider (SP);

[0092] **FIG. 24** is a diagram illustrating a verification process performed by a user device storing an IDC and a PKC;

[0093] **FIG. 25** is a diagram illustrating a system in which verification is performed by transmitting a person identification certificate (IDC) stored in a personal terminal such as an IC card to a shared user device;

[0094] **FIG. 26** is a diagram illustrating a system in which verification is performed by decrypting a person identification certificate (IDC) stored in a personal terminal such as an IC card and then transmitting the decrypted IDC to a shared user device;

[0095] **FIG. 27** is a diagram illustrating a system in which verification is performed by a personal terminal such as an IC card using a person identification certificate (IDC) stored

in the personal terminal and only the result of the verification is transmitted to a shared user device;

[0096] **FIG. 28** is a diagram illustrating a process performed when template information of a person identification certificate (IDC) is encrypted using a public key of a service provider (SP);

[0097] **FIG. 29** is a diagram illustrating a system in which verification is performed by transmitting a person identification certificate (IDC) stored in a user device to a service provider (SP);

[0098] **FIG. 30** is a diagram illustrating a system in which verification is performed by decrypting a person identification certificate (IDC) stored in a user device and then transmitting the decrypted IDC to a service provider (SP);

[0099] **FIG. 31** is a diagram illustrating a system in which verification is performed by a user device using a person identification certificate (IDC) stored in the user device and only the result of the verification is transmitted to a service provider (SP);

[0100] **FIG. 32** is a diagram illustrating a configuration of a secure container containing a content to be distributed via content transaction;

[0101] **FIG. 33** is a diagram illustrating a form of a list of person identification certificates (IDCs);

[0102] **FIG. 34** is a diagram illustrating a specific example of a form of sales restriction (UCP) information;

[0103] **FIG. 35** is a diagram illustrating an example of a format of a permitted usage data;

[0104] **FIG. 36** is a diagram illustrating an example of a data format of price information included in a secure container;

[0105] **FIG. 37** is a diagram illustrating a manner of distributing a content using a secure container;

[0106] **FIG. 38** is a diagram illustrating an example of a data format of usage control status (UCS) information;

[0107] **FIG. 39** is a diagram illustrating a manner of using a person identification certificate (IDC) when a secure container containing a content is distributed from a service provider to a user device;

[0108] **FIG. 40** is a flow chart of a process in which a secure container is received from a service provider and a person authentication is performed by a user device so that the content can be used only by authorized users;

[0109] **FIG. 41** is a flow chart of a process in which a person authentication is performed by a service provider and a secure container is distributed only to authorized users;

[0110] **FIG. 42** is a diagram illustrating a manner of distributing a content among users using a secure container;

[0111] **FIG. 43** illustrates another manner in which a content is distributed using a secure container among users and a manner in which user authentication is performed;

[0112] **FIG. 44** is a flow chart of a process in which a secure container is received from a user device A and person authentication is performed by a user device B so that only authorized users can use the content;

[0113] **FIG. 45** is a flow chart of a process in which person authentication is performed by a content distributor before distributing a content and a secure container is distributed only to authorized users;

[0114] **FIG. 46** is a block diagram mainly illustrating configurations of user devices which transmit a secure container to each other;

[0115] **FIGS. 47A and 47B** are diagrams illustrating various manners of linking a personal identification certificate (IDC) and a public key certificate (PKC) to each other;

[0116] **FIGS. 48A and 48B** are diagrams illustrating various manners of linking personal identification certificates (IDCs) and public key certificates (PKC) to one another;

[0117] **FIGS. 49A and 49B** are diagrams illustrating manners of storing a public key certificate (PKC) linked to a person identification certificate (IDC) into the person identification certificate (IDC);

[0118] **FIGS. 50A and 50B** illustrate manners of storing an identification number of a certificate into another certificate;

[0119] **FIGS. 51A and 51B** are diagrams illustrating examples of manners of management using link management data;

[0120] **FIGS. 52A and 52B** are diagrams illustrating another examples of manners of management using link management data;

[0121] **FIG. 53** is a diagram illustrating a configuration of a user device capable of performing person authentication and reproducing a content;

[0122] **FIG. 54** is a diagram illustrating a data flow in a process of downloading a content;

[0123] **FIG. 55** is a diagram illustrating the details of the data flow in the process of downloading a content;

[0124] **FIG. 56** is a diagram illustrating the details of the data flow in the process of downloading a content;

[0125] **FIG. 57** is a diagram illustrating the details of the data flow in the process of downloading a content;

[0126] **FIG. 58** is a diagram illustrating a data flow in processes of user registration, erasure of user registration, and making a service contract;

[0127] **FIG. 59** is a diagram illustrating the details of the data flow in the processes of user registration, erasure of user registration, and making a service contract;

[0128] **FIG. 60** is a diagram illustrating the details of the data flow in the processes of user registration, erasure of user registration, and making a service contract;

[0129] **FIG. 61** is a diagram illustrating the details of the data flow in the processes of user registration, erasure of user registration, and making a service contract;

[0130] **FIG. 62** is a diagram illustrating a flow of data in the process of requesting a person identification certificate (IDC), which is to be stored in a device, to be issued;

[0131] **FIG. 63** is a diagram illustrating the details of the flow of data in the process of requesting the person identification certificate (IDC), which is to be stored in the device, to be issued;

[0132] **FIG. 64** is a diagram illustrating the details of the flow of data in the process of requesting the person identification certificate (IDC), which is to be stored in the device, to be issued;

[0133] **FIG. 65** is a diagram illustrating the details of the flow of data in the process of requesting the person identification certificate (IDC), which is to be stored in the device, to be issued;

[0134] **FIG. 66** is a diagram illustrating a procedure of issuing a one-time PKC;

[0135] **FIG. 67** is a flow chart of the procedure of issuing a one-time PKC;

[0136] **FIG. 68** is a diagram illustrating a first manner of using a verification certificate;

[0137] **FIG. 69** is a flow chart of a process of using a verification certificate;

[0138] **FIG. 70** is a diagram illustrating a second manner of using a verification certificate;

[0139] **FIG. 71** is a diagram illustrating an example of a format of a verification certificate;

[0140] **FIG. 72** is a diagram illustrating a process in which person authentication is performed using a person identification certificate (IDC) which has already been registered in a person identification certificate authority (IDA), and a content is distributed in accordance with the person authentication;

[0141] **FIG. 73** is a flow chart of a process in which a content is distributed after performing person authentication using an IDC and performing mutual authentication using a PKC;

[0142] **FIG. 74** is a flow chart of a process in which a content is distributed after performing person authentication using an IDC and performing mutual authentication using a PKC;

[0143] **FIG. 75** is a flow chart of a process in which a content is distributed after performing person authentication using an IDC and performing mutual authentication using a PKC;

[0144] **FIG. 76** is a diagram illustrating a process in which person authentication is performed using a user IDC and a device PKC and also using an IDC which has already been registered in a person identification certificate authority (IDA), and then a content is distributed to a user using the device PKC;

[0145] **FIG. 77** is a flow chart illustrating a process in which person authentication is performed using a user IDC and a device PKC and also using an IDC which has already been registered in a person identification certificate authority (IDA), and then a content is distributed to a user using the device PKC;

[0146] **FIG. 78** is a flow chart illustrating a process in which person authentication is performed using a user IDC and a device PKC and also using an IDC which has already been registered in a person identification certificate authority (IDA), and then a content is distributed to a user using the device PKC;

[0147] **FIG. 79** is a diagram illustrating a person identification certificate (IDC) in which validity information (expiration date and the number of times the IDC is allowed to be used) of the person identification certificate (IDC) and also the expiration date of template information stored in the IDC are set;

[0148] **FIGS. 80A and 80B** are diagrams illustrating manners of managing the "expiration date or the number of times the IDC is allowed to be used" and the "expiration date of template" of the template information stored in a person identification certificate (IDC);

[0149] **FIG. 81** is a diagram illustrating a manner of managing the expiration date of the IDC and the expiration date of the template;

[0150] **FIG. 82** is a diagram illustrating a manner of managing the number of times the IDC is allowed to be used and the template expiration date;

[0151] **FIG. 83** is a flow chart illustrating a process of controlling the usage of an IDC in accordance with the "expiration date or number of times the IDC is allowed to be used" and "expiration date of template" described in a person identification certificate (IDC);

[0152] **FIG. 84** is a diagram illustrating a process in which when a person identification certificate (IDC) is used, if it turns out that the "IDC expiration date" has been reached, the person identification certificate (IDC) is updated;

[0153] **FIG. 85** is a diagram illustrating a process in which the expiration date of a person identification certificate (IDC) is checked at scheduled intervals, and if it turns out that the "IDC expiration date" has been reached, the IDC is updated;

[0154] **FIG. 86** is a diagram illustrating a process in which the expiration date of template information which has already been registered in a person identification certificate authority (IDA) is checked by the IDA and updated if the expiration date has been reached, after informing a user that the expiration date has been reached; and

[0155] **FIG. 87** is a diagram illustrating a process in which template information which has already been registered in a person identification certificate authority (IDA) is updated in response to an updating request from an user.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0156] The present invention is described in further detail below with reference to preferred embodiments in conjunction with the accompanying drawings.

[0157] The present invention is described below in terms of items listed below.

[0158] 1. Concepts of the Present Invention and the Outline of Certificates

[0159] 2. Encryption of Template

[0160] 3. Registration and Change of Template and Person Identification Certificate (IDC)

[0161] 4. Basic Manners of Using Person Identification Certificate (IDC)

[0162] 5. Authentication Using Person Identification Certificate (IDC)

[0163] 6. Control of Permission of Usage of Content According to User Authentication on the Basis of Person Identification Certificate

[0164] 7. Link between Person Identification Certificates (IDCS) and Public Key Certificates (PKCs)

[0165] 8. Using a Content on the Basis of Person Identification Certificate (IDC) and Public Key Certificate (PKC)

[0166] 9. One-Time Public Key Certificate (One-Time PKC)

[0167] 10. Verification Certificate

[0168] 11. Downloading of Person Identification Certificate (IDC) and Usage of a Content

[0169] 12. Setting the Validity Period of Person Identification Certificate (IDC)

[0170] [1. Concepts of the Invention and Outline of Certificates]

[0171] (1.1 Basic Concepts of the System According to the Invention)

[0172] First, basic concepts of the person authentication system according to the present invention are described. In the present invention, authentication of a person is realized using a person identification certificate (IDC). A person identification certificate (IDC) is issued for each person who wants to be certified by an identification authority (IDA), which is a reliable third-party agency, after verifying the identification of the person.

[0173] Each person identification certificate (IDC) includes information (template information) which identifies a corresponding person. Specific examples usable as personal identification information include fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information. Personal identification information other than biometric information such as a seal, a passport, a driver's license, or a card can also be used. Any combination of the personal identification information described above can also be used. Furthermore, a combination of a password and any personal identification described above may also be used. That is, information that only a person himself/herself can possess is used as the person identification information and is stored as template information wherein the template information is generally encrypted.

[0174] A person identification certificate (IDC) issued by an identification authority (IDA) is used by a registered user himself/herself, a service provider (SP) which provides a content to the registered user, or an agency or an organization (such as a settling financial institution) which needs to authenticate an user. A person identification certificate (IDC) is also issued by the person identification certificate authority (IDA) in response to a request from a user device which needs the person identification certificate (IDC) for authentication of an user. Specific examples of manners of using person identification certificates will be described in detail later.

[0175] Furthermore, in embodiments according to the present invention, a person identification certificate (IDC) is effectively used in conjunction with a public key certificate (PKC). For example, when a service provider (SP) distributes an encrypted content to an user, the service provider (SP) authenticates the user on the basis of a person identification certificate (IDC), and the service provider (SP) transmits the encrypted content to the user only when the user is verified as an authorized user, wherein the content is encrypted using a public key described in a public key certificate so that only the authorized user can decrypt the content.

[0176] **FIG. 2** is a diagram illustrating encrypted data communication performed by a person authentication system, using a public key certificate, according to the present invention. A person identification certificate (IDC) and a public key certificate (PKC) are issued by an identification authority (IDA) **201** and a certificate authority (CA) **202**, respectively, in accordance with predetermined procedures.

[0177] Encrypted data communication is performed, for example, between a user device A**205** and a service provider (SP) **203** which distributes a content. In the encrypted data communication, the service provider (SP) **203** first confirms that the user device A is used by a user A and then transmits a content after converting the content into encrypted data which can be decrypted by the user A.

[0178] The user A registers his/her personal information in the person identification certificate authority (IDA) **201**, and the person identification certificate authority (IDA) **201** issues a person identification certificate (IDC) to the user A. The service provider (SP) **203** verifies the authenticity of the user A on the basis of the person identification certificate (IDC). In this case, the service provider (SP) **203** is an entity which executes person authentication on the basis of the person identification certificate (IDC). The authentication may be performed in various manners on the basis of an identification certificate, as will be described in detail later.

[0179] The user A presents his/her public key to the certificate authority **202** and receives a public key certificate including a digital signature written by the certificate authority. After the service provider (SP) **203** authenticates the user A on the basis of the person identification certificate (IDC), the service provider (SP) **203** extracts the public key from the public key certificate of the user A and transmits a content to the user A after encrypting the content using the extracted public key. When the user A of the user device A**205** receives the encrypted content, the encrypted data is decrypted using a private key corresponding to the public key, and the decrypted data is used by the user A.

[0180] Authentication and transmission of encrypted data are also performed in a similar manner between a service provider (SP) **204** serving as a settling institution and a user device B**206**. That is, the service provider (SP) **204** authenticates the user B on the basis of an identification certificate of the user B and transmits data (such as a content or electronic settlement data) after encrypting the data using a public key certificate of the user B. In this case, the user device is an entity which executes personal authentication on the basis of the person identification certificate (IDC).

[0181] Furthermore, in data communication between the user device A**205** and the user device B**206**, authentication

of users A and B is performed on the basis of the person identification certificates of users A and B, and data is transmitted by means of encryption using the public key certificate of the use A or B.

[0182] As described above, identification certificates and public key certificates can be used in various situations in which data is transmitted. A person identification certificate can also be used singly. For example, when a user accesses secret information stored in a PC, the authenticity of the user is verified on the basis of a person identification certificate. A wide variety of entities, such as a service provider (SP), a user device, and a person identification certificate authority (IDA), execute person authentication on the basis of a person identification certificate.

[0183] In an embodiment of a system according to the present invention, as shown in **FIG. 2, a** person identification certificate (IDC) issued by a person identification certificate authority (IDA) **201** is linked with a public key certificate (PKC) issued by a certificate authority **202**. The link may be achieved by incorporating a public key certificate (PKC) into a person identification certificate or by creating group information indicating link information. Manners of forming links will be described in detail later.

[0184] In the public key cryptography described above, different keys are used by a sender and a receiver, wherein one of the keys is used as a public key which are opened for use by any unspecified user, while the other key is used as a private key which is kept secret. In the public key cryptography, unlike the symmetric key cryptography in which encryption and decryption are performed using a symmetric key, only a particular one person has a private key which should be kept secret, and thus it is easy to manage keys. An representative example of a public key encryption algorithm is the RSA (Rivest-Shamir-Adleman) encryption algorithm. In this technique, a product of two very large prime numbers (for example, 150-digit prime numbers) is used because it is difficult to factorize the product of two very large prime numbers (such as 150-digit prime numbers) into prime numbers.

[0185] In the public key cryptography, a large number of unspecified users are allowed to use the same public key, and the validity of a distributed public key is generally certified by a certificate called a public key certificate. For example, a user A creates a pair of a public key and a private key and sends the created public key to a certificate authority to acquire a public key certificate from the certificate authority. The user A opens the public key certificate to the public. An unspecified user acquires the public key from the public key certificate via a predetermined procedure and transmits, to the user A, a document or the like after encrypting it using the public key. Upon reception of the document, the user A decrypts the received document using the private key. The user A may also attach his/her signature encrypted with the private key to a document or the like, and unspecified user may verify the signature using the public key extracted from the public key certificate via the predetermined procedure. Before describing the person authentication system according to the present invention in further detail, the data structures of the public key certificate (PKC) and the person identification certificate (IDC) used in the system of the present invention are described.

[0186] (1.2 Public Key Certificate)

[0187] Public key certificates are described with reference to **FIGS. 3 and 4**. In the public key cryptography, a public key certificate is issued by a certificate authority (CA) which is also called an issuer authority (IA), wherein in response to receiving an ID and a public key from an user, the certificate authority issues a certificate after adding information such as an ID of the certificate authority and a validity period and also adding a signature of the certificate authority.

[0188] An example of a format of a public key certificate is described. In this specific example, the format is according to the public key certificate format X.509 V3.

[0189] Version indicates the version of the certificate format.

[0190] Serial Number indicates a serial number assigned by a public key issuer authority (IA) to a public key certificate.

[0191] Signature algorithm Identifier and algorithm parameters are fields in which the signature algorithm of the public key certificate and parameters thereof are described. Either the elliptic curve cryptography or the RSA can be used as the signature algorithm, wherein in the case where the elliptic curve cryptography is employed, parameters and the key length are described, while the key length is described in the case where the RSA is employed.

[0192] Issuer is a field in which the issuer of the public key certificate, that is, the name of the public key certificate issuer (IA) is described in the form of a distinguished name.

[0193] Validity is a field to describe a period during which the certificate is valid, wherein a start date and an expiration date are described.

[0194] Subject is a field in which the name of a subject or a user is described. More specifically, for example, the ID of a user device or the ID of a subject which supplies services is described.

[0195] In subject Public Key Info, algorithm and subject Public key, information about the public key of the user including the key algorithm is described.

[0196] The fields described above are defined in the public key certificate format X.509 V1, and fields described below are fields added thereto according to the public key certificate format X.509 V3.

[0197] In authority Key Identifier, key Identifier, authority Cert Issuer, authority Cert Serial Number, information which identifies the key of the public key certificate issuer (IA) is described, wherein, more specifically, a key identification number (octal number), the name of the public key issuer authority (IA), and a certificate number are described.

[0198] In subject key Identifier, identifiers are described in the case where a plurality of keys are certified in the public key certificate.

[0199] Key usage is a field to specify the purpose of the key, wherein a purpose is selected from the group consisting of (0) digital signature, (1) prevention of repudiation, (2) encryption of the key, (3) encryption of a message, (4)

distribution of a symmetric key, (5) verification of the signature of the certificate, and (6) verification of the signature of a revocation list.

[0200] In private Key Usage Period, a period is described during which the private key of the user is valid.

[0201] In certificate Polices, certificate policies of certificate authorities, that is, the public key certificate issuer authority (IA) and the registration authority (RA), are described. For example, a policy ID or a certification criterion according to the ISO/IEC9384-1 is described.

[0202] Policy Mapping is described only when a CA (public key certificate issuer (IA)) is certified, wherein mapping is described in terms of the policy of the public key certificate issuer (IA) which issues the certificate and the policy of the certificate authority which is certified.

[0203] In supported Algorithms, attributes of a directory (X.500) are defined. This field is used, in communication, to inform a receiving party of the attribute of the directory.

[0204] Subject Alt Name is a field to describe an alternative name of the subject.

[0205] Issuer Alt Name is a field to describe an alternative name of the certificate issuer.

[0206] Subject Direction Attribute is a field in which an arbitrary attribute of the user is described.

[0207] Basic Constraint is a field to describe whether the public key to be certified is used for signature of the certificate authority (public key certificate issuer authority (IA)) or is used by the user.

[0208] Name Constraints permitted Subtrees is a field to describe the area where the certificate is effective, wherein this field is used only when a certificate authority (public key certificate authority (CA) is certified.

[0209] In policy Constraints, constrains are described in terms of requirements of explicit policy ID or inhibit policy mapping for the remaining certification path.

[0210] CRL (Certificate Revocation List) Distribution Points is a filed to describe a reference point in the revocation list (**FIG. 9**) at which data is present which indicates whether the certificate of a user is revoked, wherein this field is used to confirm, when the user uses the certificate, that the certificate is not revoked.

[0211] Signature is a field in which a signature of the public key certificate issuer (public key certificate authority (IA) is written. The signature is data which is created by generating a hash value by applying a hash function to the whole of a certificate and then encrypting the resultant hash value using a public key of a certificate authority.

[0212] A certificate authority issues a public key certificate in the format shown in **FIGS. 3 and 4** and also updates a public key certificate which has expired. Furthermore, the certificate authority generates, manages, and distributes an illegal user list (revocation list) to shut out users who have made an illegal act. The certificate authority also generates a public key and a private key, as required.

[0213] When a user uses the public key certificate, the user verifies the digital signature of the public key certificate using the public key of the certificate authority the user has. If the verification of the digital signature is successfully passed, the user extracts the public key from the public key certificate. Therefore, all users, who want to use the public key certificate, need to have the common public key of the certificate authority.

[0214] (1.3 Person Identification Certificate)

[0215] Each person identification certificate (IDC) used in the person authentication system according to the present invention includes information which identifies a person (hereinafter, this person identification information included in the IDC is referred to as template information). An example of template information is biometric information of a person such as fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information. Personal identification information other than biometric information is also usable. Specific examples of such personal identification information includes a seal, a passport, a driver's license, and a card. Any combination of the personal identification information described above can also be used. Furthermore, a combination of a password and any personal identification described above may also be used. That is, information that only a person himself/herself can possess is used as the person identification information. It is desirable that the template information be stored in the IDC after being encrypted so as to prevent the template information from being leaked to an unauthorized third party. However, encryption of the template is not necessarily required if the distribution of the person identification certificate is very limited and if the template is thus prevented from being leaked.

[0216] A digital signature of a person identification authority (IDA) is written in a person identification certificate (IDC) so that the person identification certificate is prevented from being tampered with.

[0217] **FIG. 5** illustrates an example of a person identification certificate format. The person identification certificate format shown in **FIG. 5** includes indispensable item fields, extended item fields, and a signature field. The respective items are described below.

[0218] First, the respective fields of the indispensable items are described.

[0219] Version indicates the version of the certificate format.

[0220] Serial Number indicates a serial number assigned by a person identification authority (IDA) to a person identification certificate (IDC).

[0221] In Signature algorithm Identifier algorithm parameter, the signature algorithm of the person identification certificate and parameters thereof are described.

[0222] Either the elliptic curve cryptography or the RSA can be used as the signature algorithm, wherein in the case where the elliptic curve cryptography is employed, parameters and the key length are described, while the key length is described in the case where the RSA is employed.

[0223] Issuer is a field in which the issuer of the person identification certificate, that is, the name of the person identification certificate authority (IDA) is described in the form of a distinguished name.

[0224] Validity is a field to describe a period during which the certificate is valid, wherein a start date and an expiration date are described.

[0225] Subject is a field in which the name of a subject or a user is described. In this field, more specifically, the ID or the name of the user is described.

[0226] Subject Template Info is a field to describe identification information of an user, wherein data representing biometric information such as a fingerprint of the user is stored after being encrypted. More specifically, the encryption algorithm used to encrypt the template, the unique identifier (ID) or the certificate number of the public key certificate used in encryption, an encryption algorithm, a parameter, a start date and an expiration date indicating the validity period of the template, the type of the template, and the template (encrypted) are described.

[0227] The fields described above are set as the indispensable item fields.

[0228] Now, extended fields of the person identification certificate (IDC) are described.

[0229] Subject PKC info is a field to describe the public key certificate information of the subject to be certified, including the certificate number of the public key certificate of the subject and the subject unique ID of the public key certificate of the subject.

[0230] In Issuer Unique ID, the unique ID of the person identification certificate authority (IDA) is described.

[0231] In Subject Unique ID, the unique ID of the subject to be certified is described.

[0232] In Public Key Certificate, the public key certificate described above is stored.

[0233] In Issuer Alt Name, an alternative name of the person identification certificate authority is described.

[0234] In Subject Directory Attribute, an arbitrary attribute of an user, such as an age, sex, address, telephone number, is encrypted as required to identify the user.

[0235] Valid Count is a field to describe the maximum number of times the person identification certificate is allowed to be used. More specifically, after a certificate is issued, the certificate is allowed to be used as many times as described in this field.

[0236] In Control Table link Infor, group information indicating the link between the person identification certificate (IDC) and the public key certificate (PKC) is described. For example, information is described which indicates a link to a public key certificate used in data communication or data processing which is executed only when a user is successfully authenticated on the basis of the person identification certificate. The link information and the group information will be described in detail later.

[0237] The extended fields of the person identification certificate (IDC) have been described above.

[0238] The digital signature is data which is created by generating a hash value by applying a hash function to all fields of the certificate and then encrypting the resultant hash value using the public key of the person identification certificate authority (IDA).

[0239] Other information may also be described in the extended fields of the person identification certificate (IDC). For example, when the template information is encrypted using not the public key but a common private key, and the common key used in the encryption is encrypted using the public key of the user device, the service provider, or the person identification certificate authority (IDA), the encrypted public key is described in an extended field. The process performed in this case will be described later.

[0240] [2. Encryption of Template]

[0241] The person identification certificate (IDC) described above includes information (template information) used to identify a person. An example of template information is biometric information of a person such as fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information. Personal identification information other than biometric information is also usable. Specific examples of such personal identification information includes a seal, a passport, a driver's license, and a card. Any combination of the personal identification information described above can also be used. Furthermore, a combination of a password and any personal identification described above may also be used. That is, information that only a person himself/herself can possess is used as the person identification information.

[0242] It is desirable that the template be stored after being encrypted to prevent the template from being leaked to a third party, unless the distribution of the certificate is limited so as to keep a secret. The manners of encrypting and storing a template are described below.

[0243] A template may be stored and encrypted in various manners as described below.

[0244] 1) The template is stored without being encrypted.

[0245] 2) The template is encrypted using the public key of the user (identified by the person identification certificate).

[0246] 3) The template is encrypted using the symmetric key Kt, and the symmetric key Kt is encrypted using the public key of the user.

[0247] 4) The template is encrypted using a public key of a service provider (SP) (which identifies a user to which a service is to be provided, by means of using a person identification certificate).

[0248] 5) The template is encrypted using the symmetric key Kt and the symmetric key Kt is encrypted using the public key of the service provider (SP).

[0249] 6) The template is encrypted using the public key of the person identification certificate authority (IDA).

[0250] 7) The template is encrypted using the symmetric key Kt, and the symmetric key Kt is encrypted using the public key of the person identification certificate authority (IDA).

[0251] The template may be stored after being encrypted or without being encrypted in one of the above manners, each of which will be described in further detail below with reference to **FIGS. 6, 7**, and **8**. **FIG. 6A** illustrates an

example in which a template is not encrypted, and data representing biometric information such as a fingerprint acquired via a person identifying apparatus is directly stored as template information in a person identification certificate (IDC).

[0252] **FIGS. 6B** illustrate an example in which encryption and decryption are performed using only a public key, wherein in encryption shown in **FIG. 6B, a** template of a user acquired as identification information via a person identifying apparatus is encrypted using a public key of the user or a user device, a public key of a service provider (SP) (which identifies a user to which a service is to be provided, by means of using a person identification certificate), or a public key of a person identification certificate authority (IDA). Encryption may be performed in accordance with, for example, the elliptic curve cryptography (ECC) or the RSA (Rivest-Shamir-Adleman) cryptography. The encrypted template is stored in the person identification certificate (IDC), together with the identifier (unique ID) of the public key and data indicating the encryption algorithm employed in the encryption of the template.

[0253] The public key used herein is a public key which can be identified by the unique ID of the public key. The unique ID of the public key is information which can identify a public key certificate, wherein specific examples include a user ID and a user name stored in a public key certificate. The public key used herein is selected, depending upon the manner in which the person identification certificate (IDC) is used, from the group consisting of the public key of the user, the public key of the service provider (SP) (which identifies a user to which a service is to be provided, by means of using a person identification certificate), and the public key of the person identification certificate authority (IDA).

[0254] **FIG. 7** shows various manners of using a public key to encrypt a template. In the case of a person identification certificate (IDC) in which a public key of a user or a user device is used to encrypt a template, an example of usage of the person identification certificate (IDC) is to identify a particular user who is authorized to use a user device (such as a PC). When a user wants to use a PC, the template stored in the person identification certificate (IDC) is decrypted using the private key of the user and is compared with an input template to verify the authenticity of the user.

[0255] An example of usage of a person identification certificate (IDC) in which a template is encrypted using a public key of a service provider is to identify a particular user to whom a service is to be provided by the service provider. The service provider extracts the encrypted template information from a person identification certificate (IDC) of an user, which is stored in the service provider or transmitted from the user or the person identification certificate authority (IDA), and the service provider decrypts the encrypted template information using the private key of the service provider. The service provider then compares the decrypted template with sampling information (such as fingerprint data) presented by a person to be verified.

[0256] A person identification certificate (IDC) in which a template is encrypted using a public key of the person identification certificate (IDC) is used, for example, in data transmission between terminals, to identify transmitting and receiving users on the basis of the person identification certificate (IDC) issued by the person identification certificate authority (IDA). As described above, the template information is encrypted in a different manner depending upon the usage of the person identification certificate (IDC).

[0257] **FIG. 6C** shows a process of decrypting a template encrypted with a public key. An encrypted template is extracted from a person identification certificate (IDC), and then data indicating the encryption algorithm and the unique ID of a public key are extracted. Furthermore, a private key corresponding to the public key specified by the public key unique ID is extracted, and the encrypted template is decrypted using the extracted private key thereby extracting the template. Each entity which executes the person verification, such as a user device or a service provider which verifies an user, includes an encryption unit for decrypting and encrypting data.

[0258] **FIGS. 8A and 8B** are diagrams each illustrating a manner of encrypting and decrypting a template of a person identification certificate, using a symmetric key and a public key. **FIG. 8A** illustrates an encrypting process. First, for example, in a person identification certificate authority (IDA) which wants to generate encrypted template information, a symmetric key is generated using a random number, and a template input via a person identifying apparatus is encrypted using the symmetric key. Furthermore, a public key employed, that is, one of a public key of the user or of a user device, a public key of a service provider (SP), and a public key of the person identification certificate authority (IDA) is encrypted using the symmetric key. The public key is selected depending upon the usage manner described above with reference to **FIG. 7**.

[0259] The resultant encrypted template and encrypted symmetric key are stored in the person identification certificate (IDC) together with the identifier (unique ID) of the public key and the data indicating the encryption algorithm applied to the encryption of the template and the encryption of the symmetric key.

[0260] **FIG. 8B** illustrates a decrypting process using the symmetric key and the private key. The encrypted template is extracted from the encrypted template information of the person identification certificate (IDC). Furthermore, the encrypted symmetric key, the data indicating the encryption algorithm, and the public key unique ID are extracted. The encrypted symmetric key is decrypted using the private key specified by the public key specified by the public key unique ID, and the encrypted template is decrypted using the symmetric key obtained via the above decryption process, thereby extracting the template.

[0261] [3. Registration and Change of Template and Person Identification Certificate (IDC)]

[0262] Processes of registering, deleting, changing, adding, suspending, and canceling of suspension of a person identification certificate (IDC) in which data is described in the above-described manner are described below. Herein, the suspending of an IDC is a process of temporarily invalidating the IDC, and the canceling of suspension is a process of re-validating the temporarily suspended IDC.

[0263] (3.1 Registration of Template)

[0264] To effectively register a person identification certificate (IDC), a person to be certified with a person iden-

tification certificate (IDC) first presents sampling information to register his/her template. As described earlier, an example of template information is biometric information of a person such as fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information. Personal identification information other than biometric information is also usable. Specific examples of such personal identification information includes a seal, a passport, a driver's license, and a card. Any combination of the personal identification information described above can also be used. Furthermore, a combination of a password and any personal identification described above may also be used. That is, information that only a person himself/herself can possess is used as the person identification information.

[0265] **FIG. 9** illustrates a flow in terms of registration of a template and creation of an IDC. Registration of a template is performed on the basis of information (sampling information) acquired using an apparatus capable of acquiring personal information in one of the various forms described earlier. For example, in the case where fingerprint information is used as a template, a fingerprint reading apparatus is used, while a voice print acquisition apparatus is used in the case where voice print information is used as a template (S11). The acquired data is transmitted online or offline to a person identification certificate authority (IDA) (S12). A user transmits his/her personal information (PIN) identifying the user to the person identification certificate authority (IDA) (S13).

[0266] In the case where the data described above are transmitted online, mutual authentication is performed between the device of the user and the person identification certificate authority (IDA), wherein data is transmitted together with a digital signature, and the signature is verified at a receiving end. The person identification certificate authority (IDA) checks the data to confirm that the data has not been tempered with, identifies the user, and verifies the data (S14). If it is determined that the data is not valid, error handling is performed (S17) without performing registration.

[0267] In the registration of the template, the person identification certificate authority (IDA) verifies the identification of the user on the basis of user identification data which identifies the user. The person identification certificate authority (IDA) also acquires personal information such as an address or a telephone number, as required. After verifying the identification of the user and the verifying other necessary data, the person identification certificate authority (IDA) assigns a person identifier to the template and stores it in a database (S15). The person identification certificate authority (IDA) encrypts the template using the public key of the person identification certificate authority (IDA) and creates a person identification certificate (IDC) in which the encrypted template is stored (S16). The key used to encrypt the template stored in the IDC may be different depending upon the location where the IDC is used, that is, depending upon the entity which executes authentication of a person. For example, a public key of a service provider or a user device is used depending upon the situation.

[0268] (3.2 Deleting of Template)

[0269] A template registered in a person identification certificate authority (IDA) may be deleted by performing a template deleting process. The deleting process is performed in response to a deleting request issued by an user. **FIG. 10** shows a flow of the template deleting process. When a user requests deletion of a template (S21), the user submits his/her identification data which identifies the user to a person identification certificate authority (IDA) (S22). Furthermore, the user transmits his/her personal information (PIN) used for identification to the person identification certificate authority (IDA) (S23).

[0270] In the case where the data described above are transmitted online, mutual authentication is performed between the device of the user and the person identification certificate authority (IDA), wherein data is transmitted together with a digital signature, and the signature is verified at a receiving end. The person identification certificate authority (IDA) checks the data to confirm that the data has not been tempered with, identifies the user, and verifies the data (S24). If it is determined that the data is not valid, error handling is performed (S27) without performing the deleting process.

[0271] After identifying the user on the basis of the person identification data to confirm that the request has been issued by the user himself/herself (S24), the person identification certificate authority (IDA) deletes the requested template and the associated person identification data and other additional information (S25). Furthermore, the person identification certification authority (IDA) deletes the person identification certificate (IDC) in which the template was present, and registers the deleted IDC in a revocation list (S26). More specifically, the IDC identifier corresponding to the deleted IDC is registered in the revocation list.

[0272] (3.3 Changing of Template)

[0273] A template registered in a person identification certificate authority (IDA) may be changed by performing a template changing process. **FIG. 11** illustrates a flow of the template changing process. A user submits a template changing request to a person identification certificate authority (IDA) (S31), creates sampling information or the like used to create a new template (S32), and transmits identification data identifying the user and additional information (PIN) as required to the person identification certificate authority (IDA) (S33, S34). The person identification certificate authority (IDA) identifies the user on the basis of the identification data (S35), deletes the person identification certificate (IDC) based on the current template (S36), and registers the deleted IDC in the revocation list (S37). Furthermore, the person identification certificate authority (IDA) assigns an identification number to the new template and stores it in the database (S38), encrypts the template using the public key of the person identification certificate authority (IDA), and creates a person identification certificate (IDC) in which the encrypted template is stored (S39). In on-line data communication between the user device and the person identification certificate authority (IDA), mutual authentication, addition of a signature to data to be transmitted, and verification of the signature are performed in a similar manner to the processes described above.

[0274] (3.4 Addition of Template)

[0275] A user may add another identification data as an additional template to the template which has been already registered in a person identification certificate authority

(IDA). **FIG. 12** illustrates the template addition process. A user issues a template addition request to a person identification certificate authority (IDA) (**S41**), creates a new template using a template acquisition apparatus (**S42**), and transmits it together with identification data to the person identification certificate authority (IDA) (**S43**, **S44**). The person identification certificate authority (IDA) verify the received identification data (**S45**) to authenticate the user, assigns a person identifier (number) to the template to be added and stores it in the database (**S46**), encrypts the template to be added using the public key of the person identification certificate authority (IDA), and creates a person identification certificate (IDC) in which the encrypted template is stored (**S47**). In on-line data communication between the user device and the person identification certificate authority (IDA), mutual authentication, addition of a signature to data to be transmitted, and verification of the signature are performed in a similar manner to the processes described above.

[**0276**] (3.5 Suspension of Template)

[**0277**] A template registered in a person identification certificate authority (IDA) may be suspended temporarily in response to a suspension request issued from an user. **FIG. 13** illustrates a flow of a template suspension process. If a user issues a template suspension request to a person identification certificate authority (IDA) (**S51**) and submits identification data and addition data to the person identification certification authority (IDA) (**S52**, **S53**), the person identification certificate authority (IDA) identifies the user on the basis of the identification data (**S54**) and suspends the validity of the requested template of the user and the associated identification data and additional information (**S55**). In this suspension process, the person identification certificate authority (IDA) also revokes the person identification certificate (IDC) of that user and registers it in the revocation list (**S56**). More specifically, the IDC identifier corresponding to the deleted IDC is registered in the revocation list. In on-line data communication between the user device and the person identification certificate authority (IDA), mutual authentication, addition of a signature to data to be transmitted, and verification of the signature are performed in a similar manner to the processes described above.

[**0278**] (3.6 Cancellation of Suspension of Template)

[**0279**] A template whose validity was suspended via the suspension process may be re-validated in response to a suspension cancel request issued by an user. **FIG. 14** illustrates a template suspension canceling process. A user issues a template suspension cancel request to a person identification certificate authority (IDA) (**S61**) and submits identification data and additional information to the person identification certificate authority (IDA) (**S62**, **S63**). After verifying identification of the user on the basis of the identification data (**S64**), the person identification certificate authority (IDA) cancels the suspension of validity of the requested template of the user and the associated identification data and additional information (**S65**). Furthermore, the person identification certificate authority (IDA) removes the person identification certificate (IDC) of that user from the revocation list (**S66**). More particularly, the corresponding IDC identifier is removed from the revocation list. In on-line data communication between the user device and the person identification certificate authority (IDA), mutual authentication, addition of a signature to data to be transmitted, and verification of the signature are performed in a similar manner to the processes described above.

[**0280**] (3.7 Distribution of Person Identification Certificate (IDC))

[**0281**] Distribution of a person identification certificate (IDC) created on the basis of a template registered after being supplied from a user is described below.

[**0282**] **FIG. 15** illustrates a flow of a process of distributing a person identification certificate (IDC) to service providers (SPs). A service provider who wants to use a person identification certificate (IDC) makes, in advance, a contract including a rule of using IDCs with a person identification certificate authority (IDA) (**S71**). Thereafter, mutual authentication is performed between the person identification certificate authority (IDA) and the service provider (SP) (**S72**). The mutual authentication may be performed, for example, via a process using symmetric key encryption or public key encryption.

[**0283**] If a success is achieved in mutual authentication, the service provider (SP) transmits to the person identification certificate authority (IDA) a request for issuing person identification certificate (IDC) together with user identification data or data indicating the name of a user to whom a service is to be provided and also data indicating the desired policy of the person identification certificate (IDC) (**S73**). The person identification certificate authority (IDA) verifies the person identification certificate issuing request (**S74**), sets the policy of the person identification certificate (IDC) in accordance with the usage rule (**S75**), extracts the requested person identification certificate (IDC) of the user from the database, decrypts the user template encrypted with the public key of the person identification certificate authority (IDA), encrypts the user template using the public key of the service provider (**S76**), creates a person identification certificate (IDC) according to the policy (**S77**), and supplies the created IDC to the service provider (SP) (**S78**). In the case where the template stored in the database is not encrypted, or in the case where encryption is not required, the encryption of the template is not necessary.

[**0284**] (3.8 Updating of Person Identification Certificate (IDC))

[**0285**] Now, a process of updating a person identification certificate (IDC) created on the basis of a registered template of a user is described below. In most cases, updating is performed to reset the validity period of a person identification certificate (IDC) being used.

[**0286**] **FIG. 16** illustrates a flow performed in response to a person identification certificate (IDC) updating request issued from a service provider (SP). A service provider who wants to use a person identification certificate (IDC) makes, in advance, a contract including a rule of using IDCs with a person identification certificate authority (IDA) (**S81**). Thereafter, mutual authentication is performed between the person identification certificate authority (IDA) and the service provider (SP) (**S82**). The mutual authentication may be performed, for example, via a process using symmetric key encryption or public key encryption.

[**0287**] If a success is achieved in the mutual authentication, the service provider (SP) transmits to the person

identification certificate authority (IDA) a request for updating a desired person identification certificate (IDC) (**S83**). The person identification certificate authority (IDA) verifies the updating request (**S84**), sets the policy of the person identification certificate (IDC) in accordance with the usage rule (**S85**), extracts the requested person identification certificate (IDC) of the user from the database, decrypts the user template encrypted with the public key of the person identification certificate authority (IDA), encrypts the user template using the public key of the service provider, creates a person identification certificate (IDC) according to the policy (**S86**), sets the validity period, and supplies the created IDC to the service provider (SP) (**S87**). In the case where the template stored in the database is not encrypted, or in the case where encryption is not required, the encryption of the template is not necessary.

[**0288**] (3.9 Deleting of Person Identification Certificate (IDC))

[**0289**] Deleting of a person identification certificate (IDC) created on the basis of a template registered after being supplied from a user is described below.

[**0290**] **FIG. 17** illustrates a process performed in response to a person identification certificate (IDC) deleting request issued by an user. When a user wants to delete a person identification certificate (IDC), the user transmits to a person identification certificate authority (IDA) a request for deleting a particular person identification certificate (IDC) (**S91**). The person identification certificate authority (IDA) verifies the deleting request (**S92**) and deletes the specified person identification certificate (IDC) (**S93**).

[**0291**] (3.10 Inquiring About Person Identification Certificate (IDC))

[**0292**] Inquiring about a person identification certificate (IDC) created on the basis of a template registered after being supplied from a user is described below. Inquiring is performed, for example, when a service provider (SP), who does not have a person identification certificate (IDC), transmits sampling data received from a user to a person identification certificate authority (IDA) to inquire about the authenticity of the user. In response to the inquiry, the person identification certificate authority (IDA) verifies the authenticity of the user on the basis of the person identification certificate (IDC) stored in the person identification certificate authority (IDA), and the person identification certificate authority (IDA) returns only the authentication result to the service provider.

[**0293**] **FIG. 18** illustrates a flow of a process performed in response to a person identification certificate (IDC) inquiry request issued by a service provider (SP). A service provider, who wants to make an inquiry in terms of a person identification certificate (IDC), makes a contract including an usage rule of person identification certificates (IDCs) with a person identification certificate authority (IDA) (**S01**). Thereafter, mutual authentication is performed between the person identification certificate authority (IDA) and the service provider (SP) (**S02**). The mutual authentication may be performed, for example, via a process using symmetric key encryption or public key encryption.

[**0294**] If a success is achieved in the mutual authentication, the service provider (SP) transmits to the person identification certificate authority (IDA) a request for inquiry about a person identification certificate (IDC) of a particular user together with sampling data or the like of that user (**S03**, **S04**). The person identification certificate authority (IDA) verifies the inquiry request (**S05**), verifies the received sampling data on the basis of the corresponding person identification certificate (IDC) (**S06**), and transmits a verification result (OK or NG) to the service provider (SP) (**S07**).

[**0295**] [4. Basic Manners of Using Person Identification Certificate (IDC)]

[**0296**] Basic manners of using a person identification certificate (IDC) are described below. In particular, relationships between a certificate authority (CA) which issues a public key certificate (PKC), a person identification certificate authority (IDA) which issues a person identification certificate (IDC), and a device which uses those certificates are described.

[**0297**] **FIGS. 19 and 20** illustrate two examples of systems including a certificate authority (CA) which issues a public key certificate (PKC), a person identification certificate authority (IDA) which issues a person identification certificate (IDC), and a device which uses those certificates. In the example shown in **FIG. 19, a** comparison between sampling information and a template of a person identification certificate (IDC) is made by a person identification certificate authority (IDA), while a comparison between sampling information and a template of a person identification certificate (IDC) is made by a service provider (SP) or a user device (UD) in the example shown in **FIG. 20**.

[**0298**] In **FIG. 19**, the user device (UD) or the service provider (SP) **300** includes a sampling information processing unit **310** for acquiring personal information such as fingerprint data of various users and processing the acquired personal information, wherein the sampling information processing unit **310** includes a personal information acquisition unit **314** for acquiring sampling information, an information converter **313** for converting fingerprint data or the like into a code, and a communication unit **312** for transmitting the converted code to a person identification certificate authority **320**, and wherein the sampling information processing unit **310** stores a public key certificate for use in encryption/decryption of data in various communication processes. A controller **311** controls the operations of the personal information acquisition unit **314**, the information converter **313**, and the communication unit **312**.

[**0299**] The person identification certificate authority (IDA) **320** includes a comparator **321** and storage means **322**, wherein the comparator compares sampling data received from the user device (UD) or the service provider (SP) **300** with a template, stored in the storage means, of a user to be certified (preferably, the template is encrypted and stored in the person identification certificate). The storage means stores, in addition to templates, data indicating the history of issuing person identification certificates and data indicating the history of comparison.

[**0300**] A certificate authority (CA) **330** is an agency which issues a public key certificate (PKC) of a user in response to a request from the user, wherein the public key certificate includes a signature of the certificate authority. The certificate authority stores and manages data indicating the history of issuing public key certificates and the verification history.

[0301] If the person identification certificate authority (IDA) **320** receives sampling information from the user device (UD) or the service provider (SP) **300**, the person identification certificate authority (IDA) **320** compares the received sampling information with a stored template, wherein an OK or NG message is transmitted as a comparison result to the user device (UD) or the service provider (SP) **300** depending upon whether the received sampling information matches with the stored template. Herein, a verification certificate in a predetermined format may be issued, as will be described later. In the case where a verification certificate is issued, the person identification certificate authority describes the history of issuing verification certificates.

[0302] Communication among the certificate authority (CA), the person identification certificate authority (IDA) **320**, and the user device (UD) or the service provider (SP) **300** is performed only when a success is achieved in mutual authentication, wherein it is desirable that secret data be encrypted using a session key created via the mutual authentication or using public keys of two parties.

[0303] In the case of the system shown in **FIG. 20, a** comparison between sampling information and a template of a person identification certificate (IDC) is made by a service provider (SP) or a user device (UD).

[0304] The user device (UD) or the service provider (SP) **400** shown in **FIG. 20** includes a verification system **410** for acquiring personal information such as fingerprint of various users and performing verification, wherein the verification system **410** includes a general memory **413** for storing person identification certificates, a person identification certificate verification unit **414** for checking whether a person identification verification has been tempered with, a template decryption unit **415** for decrypting an encrypted template described in a person identification certificate, a personal information acquisition unit **418** for acquiring sampling information such as fingerprint data, an information converter **417** for converting fingerprint data or the like into a code, a comparator **416** for comparing the decrypted template with the coded sampling information, a communication unit **411** for communication with a person identification certificate authority **420**, and an encryption processing unit **419** including a signature generator and storing public key certificates and a public key for use in encryption/decryption of data in various communication processes. A controller **412** controls the operation of the respective units.

[0305] The person identification certificate authority (IDA) **420** includes a person identification certificate issuing unit **421** and a storage means **422**, and the person identification certificate authority (IDA) **420** issues a person identification certificate in which a template of a person to be certified is stored, in response to a request from the user device (UD) or the service provider (SP) **400**. The storage means **422** stores templates, person identification certificates, data representing the history of issuing person identification certificates, and data representing the history of verification.

[0306] A certificate authority (CA) **430** is an agency which issues a public key certificate (PKC) of a user in response to a request from the user, wherein the public key certificate includes a signature of the certificate authority. The certificate authority stores and manages data indicating the history of issuing public key certificates and the verification history.

[0307] As in the system shown in **FIG. 19**, communication among the certificate authority (CA), the person identification certificate authority (IDA) **320**, and the user device (UD) or the service provider (SP) **300** is performed only when a success is achieved in mutual authentication, wherein it is desirable that secret data be encrypted using a session key created via the mutual authentication or using public keys of two parties.

[0308] [5. Authentication Using Person Identification Certificate (IDC)]

[0309] Various manners of authentication using a person identification certificate (IDC) are described below. The authentication using a person identification certificate (IDC) can be classified into two modes described below.

[0310] (5.1 On-Line Mode)

[0311] Static IDC Verification

[0312] A template of a person identification certificate (IDC) is encrypted using a public key of a site at which verification is performed, such as a person identification certificate authority (IDA), a service provider (SP), or a user device (PC), and is registered and stored in a person identification certification authority (IDA). In response to a request from the service provider (SP) or the user device (PC), the person identification certificate authority (IDA) supplies the IDC for verification.

[0313] Dynamic IDC Verification

[0314] A template of a person identification certificate (IDC) is encrypted using a public key of a person identification certificate authority (IDA) and registered in the IDA. In response to a request from a service provider (SP) or a user device (PC), the template is re-encrypted using a public key of a site such as the SP or the PC at which verification is performed, that is, using a public key of an entity which performs person verification, and the person identification certificate (IDC) is dynamically distributed for verification.

[0315] (5.2 Off-Line Mode)

[0316] Static IDC Verification

[0317] A template of a person identification certificate (IDC) is encrypted using a public key of a site at which verification is performed, such as a person identification certificate authority (IDA), a service provider (SP), or a user device (PC), that is, using a public key of an entity which performs person verification, or a template is encrypted using a symmetric key and this symmetric key is encrypted using a public key of a person identification certificate authority (IDA), a service provider (SP) or a user device (PC) and is registered in a person identification certificate authority (IDA) and distributed to each user. When person verification is performed, an IDC and sampling information are transmitted to a site at which verification is performed. The verification processes in the respective modes are described below.

[0318] (5.1.1 On-Line Mode Static Verification)

[0319] In on-line mode static verification, when sampling data input by a person is compared, for verification, with a template of a person identification certificate (IDC), the person identification certificate (IDC) is dynamically issued by a person identification certificate authority (IDA), and

comparison for verification is performed in a system, that is, by a user device (PC), a service provider (SP), or a person identification certificate authority (IDA). That is, a comparison between sampling data input by a person and a template of a person identification certificate (IDC) is made by an entity which executes a person verification process. The person identification certificate authority (IDA) retrieves, from a database, template information encrypted with a public key of a system which performs comparison and transmits the retrieved template information to the system, at which input sampling data is compared with the template obtained by decrypting the received IDC thereby identifying the person.

[0320] **FIGS. 21A** to **21**C are diagrams illustrating manners of performing verification by a system such as a user device (such as a PC), a service provider (SP), or a person identification certificate authority (IDA). Data transfer among the respective systems including the user device, the service provider (SP), and the person identification certificate authority (IDA) shown in **FIGS. 21A** to **21**C is performed, basically, only when a success is achieved in mutual authentication between a transmitting system and a receiving device, wherein the data is transmitted after being encrypted using a session key created via the authentication process.

[0321] **FIG. 21A** shows an example in which comparison for verification is performed by a user device. A person identification certificate authority (IDA) stores a person identification certificate (IDC) including a template encrypted using a public key of the user device, wherein when the user device performs verification, the user device acquires a person identification certificate (IDC) of a person to be authenticated by requesting the person identification certificate authority (IDA) to provide the person identification certificate (IDC) of that person.

[0322] The acquisition of the person identification is performed, for example, such that the user device transmits to the person identification certificate authority (IDA) the unique ID of the public key certificate (PKC) of the user to be authenticated or the user device, and the person identification certificate authority (IDA) extracts the corresponding IDC of the person from the stored IDCs in accordance with the received unique ID and transmits the extracted IDC to the user device. Public key certificates (PKC) and person identification certificates (IDCs) may be glinked in various manners. IDC identification data depending upon the manner of forming the link is transmitted from a user device to a person identification certificate authority (IDA), and the person identification certificate authority (IDA) retrieves a person identification certificate (IDC) using the received data as a key. The manners of linking public key certificates (PKC) and person identification certificates (IDCs) will be described in further detail later.

[0323] The user device acquires a template by decrypting, using a private key of the user device, an encrypted template in a person identification certificate (IDC) received from the person identification certificate authority (IDA) and performs verification by comparing the acquired template with personal data, for example, sampling data such as fingerprint data acquired via a sampling data extracting apparatus. Depending upon whether they match with each other, verification is concluded as OK or NG. It is required that the sampling data and the template stored in the IDC should be of the same type. For example, when one of them is fingerprint data, the other one should also be fingerprint data. When one is iris data, the other should be iris data. A plurality of different identification data may be stored as templates in a person identification certificate (IDC), and input sampling data may be regarded as valid when the input sampling data matches with one of the plurality of identification data.

[0324] Only when verification is successfully passed, for example, a particular application program installed on the user device is allowed to be executed to perform data processing such as accessing to a database, updating of data, or inputting of data. If verification fails, execution of data processing is not allowed. In this case, the user device serving as a data processing apparatus having the comparison/verification capability is the entity which requests person authentication and executes person authentication.

[0325] In the system shown in **FIG. 21**B, comparison for verification is performed by a service provider (SP). A person identification certificate authority (IDA) stores a person identification certificate (IDC) including a template encrypted using a public key of the service provider (SP), wherein when the service provider performs verification, sampling information of a person to be verified and a public key certificate (PKC) of that person are transmitted to the service provider (SP) from a user device. In the case where the service provider (SP) already has the PKC, identification data identifying the PKC may be transmitted. It is desirable that sampling data be transmitted to the service provider (SP) after encrypting the sampling data using a session key created via mutual authentication or using the public key of the service provider (SP), so that the sampling data can be decrypted by only the service provider (SP). In this system, the entity which requests verification of a person is the user device, and the entity which executes the verification of the person is a service provider which provides a service to the user device.

[0326] The service provider (SP) transmits the unique ID of a public key certificate (PKC) of a person or a user device to the person identification certificate authority (IDA) to request the person identification certificate authority (IDA) to provide a person identification certificate (IDC) of the person to be verified. In accordance with the received unique ID, the person identification certificate authority (IDA) retrieves the IDC of the person from the stored IDCs and transmits the retrieved IDC to the service provider (SP). Herein, the IDC includes a template encrypted using a public key of the service provider (SP).

[0327] The service provider (SP) acquires the template by decrypting, using the private key of the service provider (SP), the encrypted template included in the person identification certificate (IDC) received from the person identification certificate authority (IDA), and the service provider (SP) performs verification by comparing the template with data which is obtained by decrypting encrypted sampling data such as fingerprint data which is acquired via a sampling data extracting apparatus and transmitted from the user device. Depending upon whether they match with each other, verification is concluded as OK or NG. The verification result (OK or NG) is transmitted to the user device, and, depending upon the verification result, it is determined

whether or not the following process such as requesting the service provider (SP) to transmit a content or requesting for viewing of data should be allowed.

[0328] In the system shown in **FIG. 21**C, comparison for verification is performed by a person identification certificate authority (IDA). The person identification certificate authority (IDA) stores a person identification certificate (IDC) including a template encrypted using a public key of the person identification certificate authority (IDA). When the person identification certificate authority (IDA) performs verification, sampling information of a person to be verified and a public key certificate (PKC) of that person or of a user device are transmitted to the person identification certificate authority (IDA) via a service provider (SP). In the case where the person identification certificate authority (IDA) already has the PKC, identification data identifying the PKC may be transmitted. It is desirable that the sampling data be transmitted to the person identification certificate authority (IDA) after being encrypted using a public key of the person identification certificate authority (IDA) so that the sampling data can be decrypted only by the person identification certificate authority (IDA). In this system, the entity which requests verification of a person is the user device or the service provider, and the entity which executes the verification of the person is the person identification certificate authority (IDA).

[0329] The person identification certificate authority (IDA) retrieves the IDC of the person of interest from the stored IDCs on the basis of the unique ID of the public key certificate (PKC) and acquires the template by decrypting the encrypted template included in the person identification certificate (IDC) using the private key of the person identification certificate authority (IDA), and furthermore, the person identification certificate authority (IDA) performs verification by comparing the template with data which is obtained by decrypting encrypted sampling data such as fingerprint data which is acquired via a sampling data extracting apparatus and transmitted from the user device via the service provider (SP). Depending upon whether they match with each other, verification is concluded as OK or NG. The verification result (OK or NG) is transmitted to the service provider (SP) and the user device, and, depending upon the verification result, it is determined whether or not the following process such as requesting by the user device the service provider (SP) to transmit a content or requesting for viewing of data should be allowed.

[0330] (5.1.2 On-Line Mode Dynamic Verification)

[0331] In on-line mode dynamic verification, when sampling data input by a person is compared, for verification, with a template of a person identification certificate (IDC), the person identification certificate (IDC) is dynamically issued by a person identification certificate authority (IDA), and comparison for verification is performed in a system, that is, by a user device (PC), a service provider (SP), or a person identification certificate authority (IDA). The template information encrypted with the public key of the person identification certificate authority (IDA) is decrypted by the person identification certificate authority (IDA) and the IDC is transmitted, after being re-encrypted using a public key of a system at which verification is to be performed, to the system, at which the template is decrypted and compared with input sampling data thereby identifying a person.

[0332] **FIG. 22** shows a system in which comparison for verification is performed by a user device. A person identification certificate authority (IDA) stores a person identification certificate (IDC) including a template encrypted using a public key of the person identification certificate authority (IDA), wherein when the user device performs verification, the user device acquires a person identification certificate (IDC) of a person to be authenticated by requesting the person identification certificate authority (IDA) to provide the person identification certificate (IDC) of that person.

[0333] In the process of acquiring the person identification certificate (IDC), a public key certificate (PKC) of a person to be certificated or of a user device, or the unique ID of the public key certificate (PKC) if the person identification certificate authority (IDA) already has the public key certificate (PKC) of that user or the user device, is transmitted to the person identification certificate authority (IDA) from the user device, and the person identification certificate authority (IDA) retrieves the IDC of the person from the stored IDCs on the basis of the received unique ID or the unique ID extracted from the PKC.

[0334] The person identification certificate authority (IDA) decrypts the encrypted template extracted from the retrieved IDC using the private key of the person identification certificate authority (IDA), re-encrypts the template using the public key of the user device, re-issues the person identification certificate (IDC), and transmits the re-issued IDC to the user device.

[0335] The user device acquires the template by decrypting, using the private key of the user device, the encrypted template included in the person identification certificate (IDC) received from the person identification certificate authority (IDA), and the user device performs verification by comparing the acquired template with personal data, for example, sampling data such as fingerprint data acquired via a sampling data extracting apparatus. Depending upon whether they match with each other, verification is concluded as OK or NG. Only when verification is successfully passed, for example, a particular application program installed on the user device is allowed to be executed to perform data processing such as accessing to a database, updating of data, or inputting of data. If verification fails, execution of data processing is not allowed.

[0336] **FIG. 23** shows a system in which comparison for verification is performed by a service provider (SP). A person identification certificate authority (IDA) stores a person identification certificate (IDC) including a template encrypted using a public key of the person identification certificate authority (IDA). When verification is performed in the service provider (SP), the service provider (SP) transmits a public key certificate (PKC) of the service provider (SP) to the person identification certificate authority (IDA). In the case where the person identification certificate authority (IDA) already has the PKC of the service provider (SP), identification data identifying the PKC may be transmitted.

[0337] Thereafter, a public key certificate (PKC) of a person to be verified or of a user device is transmitted from the user device to the person identification certificate authority (IDA) via the service provider (SP). In the case where the person identification certificate authority (IDA) already has the PKC of the user device, identification data identifying the PKC may be transmitted.

[0338] The person identification certificate authority (IDA) retrieves the IDC of the person from the stored IDCs on the basis of the received unique ID and decrypts the encrypted template included in the retrieved IDC, using the private key of the person identification certificate authority (IDA), re-encrypts the template using the public key of the service provider (SP), re-issues the person identification certificate (IDC), and transmits the re-issued IDC to the service provider (SP).

[0339] The service provider (SP) acquires the template by decrypting, using the private key of the service provider (SP), the encrypted template included in the person identification certificate (IDC) received from the person identification certificate authority (IDA), and the service provider (SP) performs verification by comparing the template with data which is obtained by decrypting encrypted sampling data such as fingerprint data which is acquired via a sampling data extracting apparatus and transmitted from the user device. Depending upon whether they match with each other, verification is concluded as OK or NG. The verification result (OK or NG) is transmitted to the user device, and, depending upon the verification result, it is determined whether or not the following process such as requesting a service provider (SP) to transmit a content or requesting for viewing of data should be allowed.

[0340] (5.2 Off-Line Mode)

[0341] In the off-line mode, verification is performed statically, unlike the on-line mode in which a person identification certificate authority (IDA) dynamically issues a person identification certificate (IDC) when the IDC is required in verification of sampling information. Therefore, person authentication is performed in a different manner depending upon the encryption algorithm used to encrypt the template information included in the person identification certificate (IDC) and also depending upon the location where comparison for verification is performed. In the off-line mode, because an encrypted template included in a person identification certificate (IDC) is decrypted by a device such as a user device or a service provider (SP) which performs comparison for verification, it is necessary that the encryption of the template be performed such that the user device or the service provider (SP) can decrypt the encrypted template.

[0342] In the off-line mode, static verification is performed as described below.

[0343] (5.2.1) Verification Performed by Device

[0344] a. Verification is performed by a user device in which both a person identification certificate (IDC) and a public key certificate (PKC) are stored.

[0345] b. Verification is performed by a user device in which both a person identification certificate (IDC) and a public key certificate (PKC) are not stored.

[0346] (5.2.2) Verification Performed by Service Provider

[0347] c. Verification is performed by a service provider when template information included in a person identification certificate (IDC) is encrypted using a public key of the service provider (SP).

[0348] d. Verification is performed by a service provider when template information included in a person identification certificate (IDC) is encrypted using a public key of a user device or a symmetric key.

[0349] The manners of verification are described below in further detail below.

[0350] (5.2.1) Verification Performed by Device

[0351] a. In the case where verification is performed by a user device in which both a person identification certificate (IDC) and a public key certificate (PKC) are stored.

[0352] A user device can include both an IDC and a PKC, for example, when the user device is designed to execute a process of comparing sampling information with a template included in a person identification certificate (IDC), provided that a person identification certificate (IDC) of a user to be authenticated and a public key certificate (PKC) exist, template information included in the person identification certificate (IDC) is encrypted using a public key of the device described in the public key certificate (PKC), and the public key certificate (PKC) can be specified by the person identification certificate (IDC). When comparison for verification is performed, the encryption algorithm of the template included in a person identification certificate (IDC) and a public key certificate (PKC) describing a public key used as an encryption key are detected, and a private key corresponding to the detected public key is then detected and the template is decrypted using the private key.

[0353] **FIG. 24** is a diagram illustrating a verification process performed by a user device storing an IDC and a PKC. The user device inputs personal data, that is, sampling information such as fingerprint information acquired via a sampling information acquisition apparatus. The user device reads a person identification certificate (IDC) stored in the user device and detects a public key certificate (PKC) in which the public key applied to the encryption of the template is stored, on the basis of the information about the template encryption algorithm. Furthermore, the user device detects the private key corresponding to the detected public key. The private key is one element of a pair of the public key and the private key of the user device, and is stored in the secure memory of the user device. Using this private key stored in the secure memory, the encrypted template of the person identification certificate (IDC) is decrypted. Thereafter, the decrypted template is compared with the sampling information.

[0354] Only when verification is successfully passed, for example, a particular application program installed on the user device is allowed to be executed to perform data processing such as accessing to a database, updating of data, or inputting of data. If verification fails, execution of data processing is not allowed.

[0355] b. In the case where an IDC and a PKC are not stored in the same device

[0356] In the case where a device is used by a great number of users (that is, in the case of a shared user device), it is difficult to store person identification certificates (IDCs) of all users in the device. In such a case, the person identification certificate (IDC) of each user is transferred into the user device from a personal terminal (such as an IC card or other mobile terminal), the process is performed on

the basis of the transferred IDC. The process is performed in one of three manners described below.

[0357] (b-1) IDC stored in a personal terminal is transmitted to a shared user device to perform verification.

[0358] (b-2) Template information is decrypted by a personal terminal and transmitted to a shared user device to perform verification.

[0359] (b-3) Verification is performed by a personal terminal.

[0360] The processes in the respective modes are described below.

[0361] (b-1) IDC stored in a personal terminal is transmitted to a shared user device to perform verification.

[0362] **FIG. 25** is a diagram illustrating a system in which verification is performed by transmitting a person identification certificate (IDC) stored in a personal terminal such as an IC card to a shared user device.

[0363] When a user wants to execute some data processing using an application program installed on the shared user device, the user inserts a mobile terminal such as an IC card into the shared user device. A person identification certificate (IDC) issued by a person identification certificate authority (IDA) is stored in the IC card. In this mode, the shared user device is an entity which executes a person verification process.

[0364] After inserting the mobile personal terminal such as an IC card into the shared user device, the person identification certificate (IDC) is transmitted from the mobile terminal to the shared user device. It is desirable that, before transmitting the IDC, mutual authentication be performed between the mobile terminal and the shared user device and the IDC is transmitted after being encrypted using a session key created in the mutual authentication process.

[0365] Upon receiving the person identification certificate (IDC) from the mobile terminal, the shared user device verifies the signature of the person identification certificate authority (IDA) added to the IDC to check whether the IDC is tampered with. If it is determined that the IDC has not been tampered with (OK), the encrypted template information is extracted from the IDC. Note that the encryption of the template was performed using the public key of the shared user device or the symmetric key. In the case where the template was encrypted using the public key of the shared user device, the template can be decrypted using the private key of the shared user device.

[0366] In the case where the template was encrypted using the symmetric key, the process described in blocks surrounded by a broken line in **FIG. 25** is performed by the personal terminal. The symmetric key used to encrypt the template is encrypted using a public key of the personal terminal and stored in a person identification certificate (IDC). The personal terminal extracts the encrypted symmetric key from the person identification certificate (IDC) and decrypts the symmetric key using the private key of the personal terminal. The obtained symmetric key is transmitted to the shared user device. It is desirable that the symmetric key be transmitted after being encrypted using a session key created during the mutual authentication. Alternatively, the symmetric key may be transmitted after being encrypted using the public key of the user device.

[0367] The shared user device decrypts the encrypted template using the private key of the shared user device and the symmetric key, and compares the template with sampling information input via the sampling information acquisition apparatus.

[0368] (b-2) In the case where template information is decrypted by a personal terminal and transmitted to a shared user device to perform verification.

[0369] **FIG. 26** is a diagram illustrating a system in which verification is performed by decrypting a person identification certificate (IDC) stored in a personal terminal such as an IC card and then transmitting the decrypted IDC to a shared user device.

[0370] After a user inserts a mobile personal terminal such as an IC card into a shared user device, a person identification certificate (IDC) decrypted by the mobile terminal is transmitted to the shared user device. Herein, the IDC includes template information which is encrypted with a public key assigned to the particular mobile terminal of each user such that the encrypted template information can be decrypted using a private key assigned to each mobile terminal. The encrypted template information extracted from the IDC is decrypted using the private key assigned to the mobile terminal and transmitted to the user device. It is desirable that, before transmitting the template, mutual authentication be performed between the mobile terminal and the shared user device and the template is transmitted after being encrypted using a session key created in the mutual authentication process. Alternatively, the template may be transmitted after being encrypted using the public key of the user device.

[0371] Upon receiving the template from the mobile terminal, the shared user device extracts the template information and compares it with sampling information input via the sampling information acquisition apparatus.

[0372] (b-3) Verification performed by a personal terminal

[0373] **FIG. 27** is a diagram illustrating a system in which verification is performed by a personal terminal such as an IC card using a person identification certificate (IDC) stored in the personal terminal and only the result of the verification is transmitted to a shared user device.

[0374] When a user inserts a mobile personal terminal such as an IC card into a shared user device, an encrypted template included in a person identification certificate (IDC) is decrypted by the mobile terminal. Herein, the IDC includes template information which is encrypted with a public key assigned to the particular mobile terminal of each user such that the encrypted template information can be decrypted using a private key assigned to each mobile terminal. The encrypted template information extracted from the IDC is decrypted using the private key assigned to the mobile terminal.

[0375] Sampling information is acquired via a sampling information acquisition apparatus and transmitted to the personal terminal such as an IC card via the user device. It is desirable that, before transmitting the sampling information, mutual authentication be performed between the

mobile terminal and the shared user device and the sampling information is transmitted after being encrypted using a session key created in the mutual authentication process. Upon receiving the sampling information from the user device, the personal terminal compares the decrypted template with the sampling information and returns the comparison result to the user device. In this mode, the IC card employed as the mobile terminal is an entity which executes a person verification process.

[0376] (5.2.2) Verification Performed by Service Provider

[0377] Manners in which a service provider (SP) authenticates an use to whom a service is to be provided are described below.

[0378] c. Verification performed by a service provider when template information included in a person identification certificate (IDC) is encrypted using a public key of the service provider (SP).

[0379] First, a process performed when template information of a person identification certificate (IDC) is encrypted using a public key of a service provider (SP) is described below with reference to **FIG. 28**.

[0380] A user device, which wants to receive a service such as content distribution or settlement from a service provider (SP), acquires a personal information such as a fingerprint of a user via a sampling information acquisition apparatus. Thereafter, mutual authentication is performed between the user device and the service provider (SP). If the mutual authentication is successfully completed, the user device transmits the sampling information to the service provider (SP). In the transmission of the sampling information, the sampling information is encrypted using a session key created during the mutual authentication or using a public key of the service provider. Furthermore, the user device transmits a person identification certificate (IDC) of the user device to the service provider (SP). The person identification certificate (IDC) includes template information encrypted using the public key of the service provider.

[0381] Upon receiving the sampling information and the person identification certificate (IDC) from the user device, the service provider (SP) decrypts the encrypted template information stored in the person identification certificate (IDC), using the private key of the service provider (SP) and compares the decrypted template information with the sampling information.

[0382] If they match with each other, the user is regarded as an authorized user, and the service provider provides a service such as content distribution or settlement to the user (user device). In the case where the verification by comparison fails, the user is regarded as an unauthorized user, and service is not provided.

[0383] d. Verification performed by a service provider when template information included in a person identification certificate (IDC) is encrypted using a public key of a user device or a symmetric key.

[0384] When template information included in a person identification certificate (IDC) is encrypted using a public key of a user device or a symmetric key, user authentication may be performed by a service provider (SP) as described below. In this case, user authentication may be performed in one of the three modes described below.

[0385] (d-1) A symmetric key used by a user device to encrypt a template is transmitted to a service provider (SP) and the service provider (SP) performs comparison for verification.

[0386] (d-2) Template information is decrypted by a user device and transmitted to a service provider (SP) for use in verification.

[0387] (d-3) Comparison for verification is performed by a user device.

[0388] The processes in the respective modes are described below.

[0389] (d-1) IDC stored in a user device is transmitted to a shared user device, and the shared user device performs comparison for verification.

[0390] **FIG. 29** is a diagram illustrating a system in which a person identification certificate (IDC) stored in a user device is transmitted to a service provider (SP) and the service provider (SP) performs comparison for verification.

[0391] When a user of a user device wants to receive a service from a service provider (SP), mutual authentication between the user device and the service provider (SP) is performed. If the mutual authentication is successfully completed, a person identification certificate (IDC) of the user is transmitted to the service provider. In the transmission of the IDC, the IDC is preferably encrypted using a session key created during the mutual authentication or using a public key of the service provider (SP).

[0392] Upon receiving the person identification certificate (IDC) from the user device, the service provider (SP) verifies a signature of a person identification certificate authority (IDA) written in the IDC to check whether or not the IDC has been tampered with. If it is determined that the IDC has not been tampered with (OK), the service provider (SP) extracts encrypted template information from the IDC, wherein a symmetric key is used in encryption of the template.

[0393] The symmetric key used to encrypt the template has been encrypted using the public key of the user device and stored in the person identification certificate (IDC). The user device extracts the encrypted symmetric key from the person identification certificate (IDC) and decrypts it using the private key of the user device. The obtained symmetric key is transmitted to the service provider (SP). It is desirable that the symmetric key be transmitted after being encrypted using a session key created during the mutual authentication. Alternatively, the symmetric key may be transmitted after being encrypted using the public key of the service provider (SP).

[0394] The service provider (SP) acquires the symmetric key by performing decryption using the private key of the service provider (SP) or the session key, and the service provider (SP) further decrypts the encrypted template using the acquired symmetric key. The service provider (SP) then compares the obtained template with sampling information which is input via a sampling information acquisition apparatus and transmitted therefrom via the user device. Mutual authentication is performed between the user device and the service provider (SP). If the mutual authentication is successfully completed, the user device transmits the sampling information to the service provider (SP). In the transmission

of the sampling information, the sampling information is encrypted using a session key created during the mutual authentication or using a public key of the service provider.

[0395] (d-2) Template information is decrypted by a user device and transmitted to a service provider (SP) for use in verification.

[0396] **FIG. 30** is a diagram illustrating a system in which verification is performed by decrypting a person identification certificate (IDC) stored in a user device and then transmitting the decrypted IDC to a service provider (SP).

[0397] A person identification certificate (IDC) is decrypted by a user device and transmitted to a service provider (SP). Herein, the IDC includes template information which is encrypted with a public key assigned to the particular user device such that the encrypted template information can be decrypted using a private key assigned to the user device. The encrypted template information extracted from the IDC is decrypted using the private key assigned to the user device, and then transmitted to the service provider (SP). It is desirable that, before transmitting the template, mutual authentication be performed between the user device and the service provider (SP) and the template is transmitted after being encrypted using a session key created in the mutual authentication process. Alternatively, the template may be transmitted after being encrypted using a public key of the service provider (SP).

[0398] Upon receiving the template from the user device, the service provider (SP) extracts the template information and compares it with sampling information which is input via a sampling information acquisition apparatus and transmitted from the user device.

[0399] (d-3) Comparison for verification is performed by a user device.

[0400] **FIG. 31** is a diagram illustrating a system in which verification is performed by a user device using a person identification certificate (IDC) stored in the user device and only the result of the verification is transmitted to a service provider (SP).

[0401] The user device decrypts the encrypted template included in the person identification certificate (IDC). Herein, the IDC includes template information which is encrypted with a public key assigned to the particular user device such that the encrypted template information can be decrypted using a private key assigned to the user device. The encrypted template information extracted from the IDC is decrypted using the private key assigned to the user device.

[0402] Sampling information is acquired via a sampling information acquisition apparatus and input to the user device. The user device performs verification by comparing the decrypted template with the sampling information and transmits the verification result to the service provider (SP). In accordance with the result, the service provider (SP) determines whether or not a service should be provided.

[0403] [6. Control of Permission of Usage of Content According to User Authentication on the Basis of Person Identification Certificate]

[0404] A process of controlling permission of usage of various contents such as music data or image data and various programs such as a game in accordance with user authentication on the basis of a person identification certificate (IDC) is described below.

[0405] **FIG. 32** illustrates a configuration of a secure container containing a content to be distributed via content transaction. The secure container shown in **FIG. 32** may be used to distribute a content from a service provider to a user device and may also be used to distribute a content from a user device to another user device.

[0406] A secure container can be distributed not only from a service provider to users but also among users. When a content is distributed among users, the distribution may be performed in either one of the two manners described below. In a first manner, a content is transmitted for sales in series from one user to another, for example, from a user A to a user B and then from the user B to a user C, and so on. The series distribution of contents among users is referred to as "intergeneration distribution". In a second manner, a content purchased by a user A is distributed in parallel from the user A to an users B, C, D, etc. That is, the same content is distributed from one user to a plurality of users. This parallel content distribution is referred to as "secondary distribution".

[0407] As shown in **FIG. 32, a** secure container **700** includes a content **701** encrypted using a content key, price information **702** including information about the price of the content, sales restriction information (USP) **703** indicating the restriction on the usage of the content, and a digital signature **704** of a producer of the secure container, such as a service provider, wherein the sales restriction information (UCP) **703** indicates, for example, that the content is permitted to be used only once and reselling among users via "intergeneration distribution" or "secondary distribution" is not permitted, or that the content is permitted to be resold among users a plurality of times. In the case where the content is permitted to be resold among users a plurality of times, the sales restriction information (UCP) **703** may indicate the details of the restriction on the reselling. For example, the sales restriction information (UCP) **703** indicates that "intergeneration distribution" is allowed up to two times or that "secondary distribution" is allowed up to three times. The price information **702** and the sales restriction information (UCP) **703** of the secure container are generically referred to as container information. At least either one of or both of the price information **702** and the sales restriction information (UCP) **703** of the container information of the secure container include a list of person identification certificates (IDCs) of users who are authorized to use the content.

[0408] **FIG. 33** is a diagram illustrating a form of a list of person identification certificates (IDCs). The list of person identification certificates (IDCs) includes user IDs or user identifiers and identifiers of the person identification certificates (IDCs) of the respective users.

[0409] The container information including the price information **702** and the sales restriction information (UCP) **703** is management information which is set by one of a content producer, a content provider, and a service provider. For example, a service provider produces data such that a list of person identification certificates (IDCs) of registered users is included in the price information **702** or the sales restriction information **703**. The digital signature is written

by an agency or an organization which manages the distribution of contents. In the case where the distribution of contents is managed by a service provider, the digital signature is written by the service provider.

[0410] **FIG. 34** illustrates a specific example of a form of sales restriction information (UCP) **703**. As shown in **FIG. 34**, the sales condition information (UCP) includes a person identification certificate (IDC) list **711** which is data indicating of a list of identifiers of person identification certificates (IDCs) of users who are permitted to use a content. The sales condition information (UCP) further includes a content identifier (ID), usable device conditions indicating user devices on which the content can be used, an area code indicating an area where the content can be used, and the type of permitted usage indicating the manners in which the content is permitted to be used (for example, the maximum number of times the content is allowed to be reproduced, the maximum number of time the content is allowed to be copied (downloaded)).

[0411] The type of permitted usage is data indicating the manners in which the content is permitted to be used. **FIG. 35** illustrates an example of a format of the permitted usage data. Rule numbers are assigned to respective items of the permitted usage, such as whether reproduction is permitted, whether copying is permitted, how long the copy is allowed to be reproduced or copied, and how many times the copy is allowed to be reproduced or copied. In **FIG. 35**, SCMS is copy restriction information which indicates the maximum number of times the content is allowed to be copied. A user is permitted to reproduce and copy the content within the restriction defined in the sales restriction information of the secure container, wherein the respective items of the restriction are denoted by the rule numbers.

[0412] As shown in **FIG. 34**, the sales restriction information (UCP) also includes "UCP generation management information"**712** indicating the maximum number of times the content is permitted to be distributed among user devices via "intergeneration distribution", and "maximum allowable number of secondary distributions"**713** indicating the maximum number of times the content is permitted to be distributed via "secondary distribution". The maximum number of times the content is permitted to be distributed among users defined in "UCP generation management information" is inherited into the usage control status (UCS) information **(FIG. 38)** stored in a user device depending upon the usage of the secure container. In accordance with the maximum number of times the content is permitted to be distributed among users defined in "UCP generation management information", "UCS generation management information" and "UCS allowable number of secondary distributions" are described in the usage control status (UCS) information. The "UCS generation management information" is updated each time intergeneration distribution of the content is performed and the "UCS allowable number of secondary distributions" is updated each time secondary distribution of the content is performed. The usage control status (UCS) information will be described in further detail later.

[0413] **FIG. 36** is a diagram illustrating an example of a data format of price information included in a secure container. The price information includes information indicating the content ID as in the sales restriction information (UCP) shown in **FIG. 34**. In addition, the price information includes information indicating a price information ID and information indicating a price information version. Furthermore, as in the sales restriction information (UCP) shown in **FIG. 34**, the price information includes a person identification certificate (IDC) list **721**. That is, data indicating the list of identifiers of person identification certificates (IDCs) of users who are permitted to use the content is included in the sales restriction information (UCP).

[0414] **FIG. 37** is a diagram illustrating a manner of distributing a content using a secure container. A content provider (CP) **801** generates or acquires a content which is to be stored in a secure container, and the content provider (CP) **801** provides the generated or acquired content together with sales restriction (UCP) data of the content to a service provider (SP) **802** which distributes the content to users. The service provider (SP) **802** generates price information of the content and stores a list of person identification certificates (IDC) of users who are permitted to use the content into at least one of or both of the price information and the sales restriction information (UCP). The service provider (SP) **802** further writes a digital signature thereby forming a secure container and transmits the resultant secure container to a user device **803**.

[0415] The user device **803** verifies the signature of the secure container. Furthermore, the user device **803** verifies other information such as the sales restriction (UCP) data and the price information included in the secure container to check that the data has not been tampered with. The user device **803** then extracts the IDC identifier of the user device **803** from the person identification certificate (IDC) list from either the sales restriction (UCP) data or the price information, and acquires the person identification certificate (IDC) indicated by the IDC identifier. The user device **803** then compares the template included in the IDC with sampling information. The comparison for verification is performed by one of the user device, the service provider, and the person identification certificate authority (IDA). In the case where the person verification has been successfully passed, it becomes possible for the user to use the content, that is, decrypt the content. More specifically, provided that the verification has been passed, the content key used to encrypt the content is transmitted from the service provider to the user device. This makes it possible for the user device to reproduce and copy the content included in the secure container using the content key.

[0416] The user device stores the secure container onto a storage medium of the user device **803**. The user device **803** then generates charge information indicating the charge for use of the content and transmits it to a clearing center **804** which performs settlement. The charge information is generated on the basis of the data described in the price information described earlier. The clearing center transfers the charge from, for example, an electronic money account from the user in accordance with the charge information. The user device **803** is allowed to distribute the secure container to another user device **805**, as will be described in detail later. When storing the secure container, the user devices **803** and **805** generate usage control status (UCS) information and store it into a memory.

[0417] **FIG. 38** illustrates an example of usage control status (UCS) information which is generated by a user device and stored in a memory of a user device, when the

secure container is stored. As shown in **FIG. 38**, the usage control status (UCS) information includes, in addition to the data indicating the content ID and the service provider ID, information indicating the content usage restriction such as the number of times the content is allowed to be further reproduced or the number of times the content is allowed to be further copied. Note that the number of times the content is allowed to be further reproduced or copied indicates the number of times the content is allowed to be further reproduced or copied using the same user device. The usage control status (UCS) information is generated, updated, and inherited in accordance with the permitted usage data which is included in the sales restriction (UCP) data of the content and which defines the permitted usage of the content. Thus, a user device uses the content in accordance with the content usage restriction data included in the content sales restriction (UCP) data indicating the content usage restriction or in accordance with the usage control status information generated in accordance with the usage restriction data.

[**0418**] The usage control status (UCS) information further includes a person identification certificate (IDC) list **731**. That is, data indicating the list of identifiers of person identification certificates (IDCs) of users who are permitted to use the content is included in the usage control status (UCS) information. This list is generated by inheriting the data described in the sales restriction (UCP) information. The usage control status (UCS) information further includes "UCS generation management information"**732** and "UCS allowable number of secondary distributions"**733**.

[**0419**] As described earlier, the "UCS generation management information" indicates the number of times intergeneration distribution of the content is allowed to be performed. For a user device which first purchases a content, the same number as the number defined in the "UCP generation management information" is set in the UCS generation management information. For a user device which receives the content from a user via the intergeneration distribution, the number equal to the value obtained by subtracting the number of times intergeneration distribution has been performed from the number defined in the "UCP generation management information" is set in the UCS generation management information.

[**0420**] "UCP allowable number of secondary distributions"**733** is a field in which the number of times secondary distribution of the content is allowed. For a user device which first purchases the content, the same number as the number defined in the "UCP allowable number of secondary distributions" in the sales restriction (UCP) information is set, and is updated, that is, decremented, each time secondary distribution is performed thereafter.

[**0421**] As described above, distribution of the content among users is allowed or forbidden depending upon the "UCS generation management information" or "UCS allowable number of secondary distributions" in the usage control status (UCS) information stored in the memory of the user device together with the content. The "UCS generation management information" is updated each time intergeneration distribution of the content is performed, and the "UCS allowable number of secondary distributions" is updated each time secondary distribution of the content is performed.

[**0422**] **FIG. 39** is a diagram illustrating a manner of using a person identification certificate (IDC) when a secure container containing a content is distributed from a service provider to a user device.

[**0423**] First, a user **820** of a user device **810** request a person identification certificate authority (IDA) **830** to issue a person identification certificate (IDC) of the user **820**. When the user **820** issues the request, the user **820** presents his/her biometric information and other personal information to the person identification certificate authority (IDA) **830**. After verifying the authenticity of the user, the person identification certificate authority (IDA) **830** generates template information in accordance with sampling information and further generates a person identification certificate (IDC) in which encrypted template information is stored.

[**0424**] In response to a request, the generated person identification certificate (IDC) is distributed to the user device **810** or a service provider **840** and stored therein. For example, when the user **820** wants to receive a content from the service provider **840**, the service provider **840** authenticates the user **820** on the basis of the person identification certificate (IDC) stored in the service provider **840**. That is, the service provider **840** compares the sampling information received from the user with the template information included in the person identification certificate (IDC), and, if they match with each other, the service provider **840** regards the user who provided the sampling information as an authorized user corresponding to the person identification certificate (IDC) and distributes the content to the user.

[**0425**] When the user **820** wants to use the user device **810**, authentication is also performed on the basis of the person identification certificate (IDC) stored in the user device **810**. That is, sampling information input by the user is compared with the template information included in the person identification certificate (IDC), and, if they match with each other, the user device **810** determines that the user who provides the sampling information is an authorized user corresponding to the person identification certificate (IDC) and permits the user to use the user device for data processing.

[**0426**] As described above, user authentication may be performed individually using a person identification certificate (IDC) by a user device or a service provider at various locations. Note that, as described earlier, the template stored in the person identification certificate (IDC) is encrypted using a public key of a system which performs comparison for verification.

[**0427**] **FIG. 40** is a flow chart of a process in which a secure container is received from a service provider and a person authentication is performed by a user device so that the content can be used only by authorized users. The respective steps in the flow are described below.

[**0428**] In step **S701**, mutual authentication is performed between a service provider and a user device. Only when the mutual authentication is successfully completed (Yes in **S702**), the service provider extracts a secure container (**S703**) and transmits the extracted secure container to the user device (**S704**). In the mutual authentication, a session key is created, and used, as required, to encrypt data which is transferred between the service provider and the user device.

[0429] The user device verifies the received secure container (S705). Herein, the verification includes the verification of the signature of the secure container itself and the signatures of the respective data such as the price information and the sales restriction (UCP) information described in the container.

[0430] If the verification of the container is successfully passed (Yes in S706), a user inputs sampling information and a user ID to the user device (S707). The user device extracts a person identification (IDC) list from the price information or the sales restriction (USP) information of the secure container (S708) and retrieves an IDC identifier corresponding to the user ID (S709). In the case where an IDC identifier corresponding to the input user ID is not found, it is determined that the user is not a user authorized by the service provider and an error is returned (No in S710). In this case, the following process is not performed.

[0431] If an IDC identifier corresponding to the input user ID is found in the person identification certificate (IDC) list (Yes in S710), a person identification certificate (IDC) is acquired on the basis of the IDC identifier (S711). More specifically, in the case where the person identification certificate (IDC) is stored in the user device, the IDC stored in the user device is employed, while the person identification certificate (IDC) is received from the person identification certificate authority (IDA) or the service provider if the IDC is not stored in the user device. A template is extracted from the acquired person identification certificate (IDC) and decrypted using the private key of the user device. The template is then compared with the sampling information for verification (S712). If the verification fails (No in S713), an error is returned and the following process is not performed. More specifically, the decryption of the content is not performed and thus the usage of the content is limited. In the case where the verification is affirmative (Yes in S713), the service provider is informed of the success of the verification, and the service provider transmits to the user device a content key to be used in decryption of an encrypted content stored in the secure container (S714). The user device decrypts the encrypted content using the content key received from the service provider and uses the content (S715).

[0432] In this system, as described above, a content stored in a secure container is allowed to be used only when a user is verified as an authorized user via a user verification process using a template of a person identification certificate (IDC), thereby preventing the content from being used by an unauthorized user.

[0433] **FIG. 41** is a flow chart of a process in which a person authentication is performed by a service provider and a secure container is distributed only to authorized users. The respective steps in the flow are described below.

[0434] In step S721, mutual authentication is performed between a service provider and a user device. In the mutual authentication, a session key is created, and used, as required, to encrypt data which is transferred between the service provider and the user device.

[0435] Only when the mutual authentication is successfully completed (Yes in S722), the service provider extracts a secure container (S723), and a user inputs sampling information and a user ID to the user device (S735) and transmits them to the service provider (S736).

[0436] The service provider extracts a person identification (IDC) list from the price information or the sales restriction information (UCP) of the secure container (S724) and retrieves an IDC identifier corresponding to the user ID (S725). In the case where an IDC identifier corresponding to the input user ID is not found, it is determined that the user is not a user authorized by the service provider and an error is returned (No in S726). In this case, the following process is not performed.

[0437] If an IDC identifier corresponding to the input user ID is found in the person identification certificate (IDC) list (Yes in S726), a person identification certificate (IDC) is acquired on the basis of the IDC identifier (S727). More specifically, in the case where the person identification certificate (IDC) is stored in the service provider, the IDC stored in the service provider is employed, while the person identification certificate (IDC) is received from the person identification certificate authority (IDA) if the IDC is not stored in the service provider. A template is extracted from the acquired person identification certificate (IDC) and decrypted using the private key of the service provider. The template is then compared with the sampling information for verification (S728). If the verification fails (No in S729), an error is returned and the following process is not performed. More specifically, distribution of the secure container is not performed. In the case where the verification is affirmative (Yes in S729), the user is regarded as an authorized user and the following process is performed. More specifically, the service provider distributes the secure container and the content key to the user device (S730).

[0438] The service provider transmits a secure container to the user device, and the user device verifies the received secure container (S731). Herein, the verification includes the verification of the signature of the secure container itself and the signatures of the respective data such as the price information and the sales restriction (UCP) information described in the container. If the verification of the container is successfully completed (Yes in S732), it becomes possible to use, on the user device, the content in the secure container.

[0439] In this system, as described above, a content is allowed to be distributed only when a user is verified as an authorized user via a user verification process using a template of a person identification certificate (IDC), thereby preventing the content from being distributed to an unauthorized user.

[0440] Manner of using a person identification certificate (IDC) in distribution of a secure container among user devices are described below.

[0441] **FIG. 42** is a diagram illustrating a manner of distributing a content between users using a secure container. A service provider (SP) generates price information of the content and stores a list of person identification certificates (IDC) of users who are permitted to use a content into at least one of or both of price information and sales restriction information (UCP). The service provider (SP) further writes a digital signature thereby forming a secure container and transmits the resultant secure container to a user device **1** (**920**).

[0442] If users **940** and **945** who want to use the user device **1** (**920**) are authorized users permitted to use the content, the IDC identifiers of the user are described in a list

of person identification certificates (IDCs) stored in price information or sales restriction (UCP) information of a secure container corresponding to the content or stored in usage control status (UCS) information which is generated by the user device and stored in the user device when the secure container is stored in the user device. When a user wants to use the content stored in the user device **1** (**920**), authentication of the user is performed on the basis of the IDC list in the secure container. That is, the user who wants to use the content is requested to input sampling information. The user device **1** (**920**) compares the input sampling information with the template included in the stored person identification certificate (IDC). Only when they match with each other, the user device **1** (**920**) permits the user to use the content.

[**0443**] As described earlier, the secure container may also be distributed among user devices. In the case where the secure container has been moved from the user device **1** (**920**) to a user device **2** (**930**), when users **940** and **945** use the content on the user device **2** (**930**), user authentication is performed on the basis of the IDC list described in the price information or sales restriction (UCP) information of the secure container or in the usage control status (UCS) information. That is, a user who wants to use the content is requested to input sampling information. The user device **2** (**930**) compares the input sampling information with the template included in the stored person identification certificate (IDC). Only when they match with each other, the user device **2** (**930**) permits the user to use the content.

[**0444**] As described above, when the secure container is moved, the person identification certificate (IDC) list which was originally stored in the price information or sales restriction (UCP) information of the secure container is maintained unchanged, and the IDC list in the usage control status (UCS) information generated in accordance with the sales restriction (UCP) information of the secure container is also maintained unchanged, thereby ensuring that the usage of the content is limited to only authorized users in accordance with the IDC list.

[**0445**] **FIG. 43** illustrates another manner in which a content is distributed using a secure container among users and a manner in which user authentication is performed. In the process shown in **FIG. 43**, usage of a user device, that is, access to the user device, is restricted in accordance with user authentication on the basis of a person identification certificate (IDC) stored in the user device, and, furthermore, use of a content is restricted in accordance with user authentication on the basis of price information, sales restriction (UCP) information, or an IDC list described in usage control status (UCS) information. That is, user authentication is performed for two different purposes.

[**0446**] Before staring to use a user device **1** (**950**), a user A and a user B present sampling information to a person identification certificate authority (IDA) **970** and request the person identification certificate authority (IDA) **970** to issue person identification certificates (IDCs) in which template information is stored in accordance with the sampling information. The issued person identification certificates (IDCs) are stored in the user device **1** (**950**).

[**0447**] When a user issues a request for usage of the user device **950**, the user device **950** performs user authentication on the basis of the person identification certificate (IDC) **955** stored in the user device **950**. That is, the user who wants to use the content is requested to input sampling information. The user device **950** compares the input sampling information with the template included in the stored person identification certificate (IDC). Only when they match with each other, the user is permitted to use the user device **1** (**950**).

[**0448**] When a user issues a request for usage of a content stored in a secure container **990**, user authentication is performed on the basis of the IDC list described in the price information or sales restriction (UCP) information of the secure container or described in the usage control status (UCS) information. When the user is not found in the IDC list or when, even if the user is found in the IDC list, the input sampling information does not match with the template information, the user is not permitted to use the content.

[**0449**] That is, a user can use the content of the secure container **990** on the user device **1** (**950**) only when the user authentication on the basis of the person identification certificate (IDC) stored in the user device **1** (**950**) is passed and furthermore when the user authentication on the basis of the IDC list described in the price information or the sales restriction (UCP) information of the secure container or described in the usage control status (UCS) information is passed.

[**0450**] The secure container is allowed to be moved among devices. In the case where the secure container has been moved to a user device **2** (**960**), user authentication on the basis of person identification certificate (IDC) stored in the user device **2** (**960**) and user authentication on the basis of the IDC list described in the price information or the sales restriction (UCP) information of the secure container or described in the usage control status (UCS) information are performed in a similar manner.

[**0451**] In the system shown in **FIG. 43**, person identification certificates (IDCs) **955** of users A and B are stored in the user device **1** (**950**) and a list **992** of users A, B, and C are stored in the secure container. Therefore, only users A and B are allowed to use the content using the user device **1** (**950**). On the other hand, person identification certificates (IDCs) **965** of users A and C are stored in the user device **2** (**960**) and a list **992** of users A, B, and C is stored in the secure container. Therefore, only users A and C are allowed to use the content using the user device **2** (**960**).

[**0452**] In the example shown in **FIG. 43**, the system is constructed on the assumption that each user device performs user authentication by comparing sampling information with a template of an IDC which is stored in the user device. When it is desirable that the device can be used by any user whose person identification certificate (IDC) has been registered in a person identification certificate authority (IDA), user authentication may be performed by comparing input sampling information with templates not only in IDCs stored in the device but also in person identification certificates (IDCs) stored in the person identification certificate authority (IDA), and users who have passed the user authentication may be allowed to use the device.

[**0453**] An example of a process of performing user authentication on the basis of a person identification certificate (IDC) in an IDC list described in a secure container before distributing the secure container among user devices

thereby restricting the usage of the content is described below with reference to the flow charts shown in **FIGS. 44 and 45**. Note that it is assumed herein that accessing to user devices is not limited.

[**0454**] **FIG. 44** is a flow chart of a process in which a secure container is received from a user device A and person authentication is performed by a user device B so that only authorized users can use the content. The respective steps in the flow are described below.

[**0455**] In step **S751**, mutual authentication is performed between a user device A and a user device B. Only when the mutual authentication is successfully completed (Yes in **S752**), the user device A extracts a secure container (**S753**) and transmits the extracted secure container to the user device B (**S754**). In the mutual authentication, a session key is created, and used, as required, to encrypt data which is transferred between the service provider and the user device.

[**0456**] The user device B verifies the received secure container (**S755**). Herein, the verification includes the verification of the signature of the secure container itself and the signatures of the respective data such as the price information and the sales restriction (UCP) information described in the container.

[**0457**] If the verification of the container is affirmative (Yes in **S756**), a user who wants to use a content inputs sampling information and a user ID to the user device B (**S757**). The user device B extracts a person identification certificate (IDC) from the usage control status (UCS) information and retrieves an IDC identifier corresponding to the user ID (**S759**). In the case where an IDC identifier corresponding to the input user ID is not found, it is determined that the user is not a user authorized by the service provider and an error is returned (No in **S760**). In this case, the following process is not performed.

[**0458**] If an IDC identifier corresponding to the input user ID is found in the person identification certificate (IDC) list (Yes in **S760**), a person identification certificate (IDC) is acquired on the basis of the IDC identifier (**S761**). More specifically, in the case where the person identification certificate (IDC) is stored in the user device B, the IDC stored in the user device B is employed, while the person identification certificate (IDC) is received from the person identification certificate authority (IDA) or the service provider if the IDC is not stored in the user device B. A template is extracted from the acquired person identification certificate (IDC) and decrypted using the private key of the user device B. The template is then compared with the sampling information for verification (**S762**). If the verification fails (No in **S763**), an error is returned and the following process is not performed. More specifically, the decryption of the content is not performed and thus the usage of the content is limited. In the case where the verification is affirmative (Yes in **S763**), the user device A is informed of the success of the verification, and the user device A transmits to the user device B a content key to be used in decryption of an encrypted content stored in the secure container (**S764**). The user device B decrypts the encrypted content using the content key received from the user device A and uses the content (**S765**).

[**0459**] In this system, as described above, a content stored in a secure container is allowed to be used only when a user is verified as an authorized user via a user verification process using a template of a person identification certificate (IDC), thereby preventing the content from being used by an unauthorized user even after a secure container has been distributed among user devices.

[**0460**] **FIG. 45** is a flow chart of a process in which person authentication is performed by a content distributor before distributing a content and a secure container is distributed only to authorized users. The respective steps in the flow are described below.

[**0461**] In step **S771**, mutual authentication is performed between a user device A and a user device B. In the mutual authentication, a session key is created, and used, as required, to encrypt data which is transferred between the service provider and the user device.

[**0462**] Only when the mutual authentication is successfully completed (Yes in **S772**), the user device A extracts a secure container (**S773**), and a user inputs sampling information and a user ID to the user device B (**S785**) and transmits them to the user device A (**S786**).

[**0463**] The user device A extracts a person identification (IDC) list from the price information, the sales restriction (UCP) information, or the usage control status (UCS) information of the secure container (**S774**) and retrieves an IDC identifier corresponding to the user ID (**S775**). In the case where an IDC identifier corresponding to the input user ID is not found, it is determined that the user is not a user authorized by the service provider and an error is returned (No in **S776**). In this case, the following process is not performed.

[**0464**] If an IDC identifier corresponding to the input user ID is found in the person identification certificate (IDC) list (Yes in **S776**), a person identification certificate (IDC) is acquired on the basis of the IDC identifier (**S777**). More specifically, in the case where the person identification certificate (IDC) is stored in the service provider, the IDC stored in the service provider is employed, while the person identification certificate (IDC) is received from the person identification certificate authority (IDA) if the IDC is not stored in the service provider. A template is extracted from the acquired person identification certificate (IDC) and decrypted using the private key of the service provider. The template is then compared with the sampling information for verification (**S778**). If the verification fails (No in **S779**), an error is returned and the following process is not performed. More specifically, distribution of a secure container and a content key is not performed. In the case where the verification is affirmative (Yes in **S779**), the user is regarded as an authorized user and the following process is performed. More specifically, distribution of a secure container and a content key to the user device B is performed.

[**0465**] If the user device B receives a secure container from the user device A, the user device B verifies the received secure container (**S781**). Herein, the verification includes the verification of the signature of the secure container itself and the signatures of the respective data such as the price information and the sales restriction (UCP) information described in the container. If the verification of the container is successfully completed (Yes in **S782**), it becomes possible to use, on the user device B, the content in the secure container.

[0466] In this system, as described above, a content is allowed to be distributed only when a user is verified as an authorized user via a user verification process performed by the user device A using a template of a person identification certificate (IDC), thereby preventing the content from being distributed to an unauthorized user.

[0467] **FIG. 46** is a block diagram mainly illustrating configurations of user devices which transmit a secure container to each other. A process of transferring a secure container, generating content usage control status (UCS) information, and storing the secure container is described with reference to **FIG. 46**.

[0468] A service provider **1810** shown in **FIG. 46** performs a first distribution (primary distribution) of a secure container. The service provider **1810** stores the content in a content database **1812** and also stores user information in a user information database **1813**. In the service provider **1810**, under the control of a controller **1811**, an encryption unit **1814** performs mutual authentication with a device to which a secure container is to be transferred and also writes a signature on data to be transferred. The encryption unit **1814** includes a memory for storing key information needed in the encryption process, the above-described public key of the public key certificate authority (CA), and the public key certificate issued by the public key certificate authority (CA). The database **1813** stores person identification certificates (IDCS) of users to whom services are provided. A user identifying apparatus **1816** performs user authentication, as required, by comparing sampling information with information described in an IDC.

[0469] The service provider **1810** transfers a secure container to a user device A**1820** via a communication unit **1815**. As described earlier, the secure container includes sales restriction (UCP) information and price information wherein a person identification certificate (IDC) list is described in at least either the sales restriction (UCP) information or the price information.

[0470] A clearing center **1840** shown in **FIG. 46** settles the charges for use of distributed contents (by processing electronic money data, for example). The clearing center **1840** includes an encryption unit **1844** which executes mutual authentication with respective devices in reception/transmission of logs and which adds a signature to data to be transmitted and verifies a signature of received data. The clearing center **1840** also includes a database **1842** in which various data such as user management data and user account management data. The encryption unit **1844** includes a memory for storing key information necessary in the encryption process, the public key of the public key certificate authority (CA), and the public key certificate issued by the public key certificate authority (CA). A controller **1841** controls the operations such as transmission/reception of data and transfer of data performed by the encryption unit during the encryption process. The database **1842** includes person identification certificates (IDC) of users to whom services are provided. A user identifying apparatus **1846** authenticates an user, as required, by comparing sampling information with information described in the IDCs.

[0471] The service provider **1810** transfers a secure container to a user device A**1820** via a communication unit **1815**. When the user device A**1820** receives the secure container via a communication unit **1827**, the user device A **1820** performs a purchasing process. In the purchasing process, user authentication is performed on the basis of the person identification certificate (IDC) stored in a storage unit **1825**. In the case where the person identification certificate (IDC) is not stored in the storage unit **1825**, user authentication may be performed by the service provider **1810**. In the user device A**1820**, under the control of a controller **1821**, an encryption unit **1822** generates a content usage control status (UCS) information in accordance with the sales restriction (UCP) information of the secure container and stores it in a memory such as a flash memory **1824**. As described earlier, the content usage control status (UCS) information includes a list inherited from the person identification certificate (IDC) list stored in the sales restriction (UCP) information.

[0472] The user device A**1820** performs a content usage charge payment process using, for example, electronic money **1828**. The encryption unit **1822** generates an usage log and transmits it to the service provider **1810** via the communication unit **1827**. The secure container received by the user device A**1820** is stored in a storage unit **1825** such as a hard disk. The service provider **1810** verifies the usage log transmitted from the user device A**1820**. After completion of the verification, service provider **1810** encrypts a content key using a session key and transmits the encrypted content key to the user device A**1820**. The user device A**1820** decrypts the encrypted content key using the session key, encrypts the content key using an unique storage key of the user device A**1820**, and stores it in the memory **1824**.

[0473] In usage of a content, such as reproduction of a content using a data reproducing unit **1826**, the user device A**1820** decrypts the content key stored in the memory **1824** using the storage key, decrypts the content in the secure container stored in the storage unit **1825** using the decrypted content key, and reproduces the content via the data reproducing unit **1826**. In order to perform the above-described decryption of the content in the secure container, it is required that, in the previous decision step, the number of times the content is permitted to be further reproduced indicated by the content usage restriction (UCS) information stored in the memory **1824** be read and the number should indicate that further reproduction is permitted.

[0474] When a secure container is transmitted from the user device A**1820** to the user device B **1830**, the user device A**1820** reads the content usage control status (UCS) information from the memory **1824**, decrypts it using the storage key via the decryption unit **1822** (decryption is unnecessary if the UCS information is not encrypted), and detects the "UCS generation management information" and "UCS allowable number of secondary distributions" described in the UCS. If it is determined that further distribution is permitted, the user device A**1820** transfers the secure container to the user device B**1830** via the communication unit **1827**. The user device B**1830** receives the secure container via the communication unit **1837** and performs a purchasing process.

[0475] When the secure container is transmitted, the user authentication described earlier is performed. The user authentication is performed by the user identifying apparatus **1829** of the user device A which transmits the secure container as described earlier with reference to the flow chart shown in **FIG. 45**, or by user identifying apparatus

1839 of the user device B which receives the secure container as described earlier with reference to the flow chart shown in **FIG. 44**. Alternatively, the user authentication may be performed by the service provider or the person identification certificate authority (IDA).

[**0476**] If the user authentication is passed, the user device B**1830** generates a content usage control status (UCS-B) information in which "UCS generation management information" and "UCS allowable number of secondary distributions" are newly set, using the encryption unit **1832** under the control of the controller **1831**, in accordance with the sales restriction (UCP) information of the secure container and in accordance with the UCS information of the user device A **1820**. The resultant content usage control status (UCS-B) is stored in the memory **1834** such as a flash memory.

[**0477**] In the generated UCS-B, the content usage history of the user device A**1820** is inherited. The "UCS generation management information" of the UCS-B is set to be smaller by one than the "UCS generation management information" of the UCS-A. The "UCS allowable number of secondary distribution" of the UCS-B is set to be smaller by one than the "UCS allowable number of secondary distribution" of the UCS-A, or newly set to be equal to the "UCP allowable number of secondary distributions" described in the secure container.

[**0478**] The user device B**1830** performs a content usage charge payment process using the electronic money **1838**. That is, an usage log is generated by the encryption unit **1832** and transmitted to the user device A**1820** via the communication unit **1837**. The secure container received by the user device B**1830** is stored in a storage unit **1835** such as a hard disk. The user device A**1820** verifies the usage log transmitted from the user device B**1830**. If the verification is passed, the user device A**1820** reads the content key from the memory **1824**, decrypts the content key using the storage key, decrypts the content key using the session key, and transmits it to the user device B**1830**. The user device B**1830** decrypts the encrypted content key using the session key, encrypts the content key using an unique storage key of the user device B**1830**, and stores it in the memory **1834**.

[**0479**] If the content is used beyond the upper limit by means of illegal tampering, the number of reception logs generated in accordance with the same secure container exceeds the number set in the "UCS generation management information" in the sales restriction (UCP) information in the secure container. As a result, when the data is transmitted to the clearing center **1840**, the data is determined to be invalid. The reception log includes, as well as information indicating the content ID, "UCP generation management information" described in the secure container. Thus, in the settlement performed by the clearing center **1840**, if the reception log indicates that the number of distributions exceeds the number set in the "UCP generation management information", the reception log is determined to be invalid. In the case where a reception log is generated on the basis of a content which is not permitted distributed among users, the reception log is regarded as invalid.

[**0480**] In usage of a content, such as reproduction of a content using a data reproducing unit **1836**, the user device B**1830** decrypts the content key stored in the memory **1834** using the storage key, decrypts the content in the secure container stored in the storage unit **1835** using the decrypted content key, and reproduces the content via the data reproducing unit **1836**. In the above-described decryption of the content in the secure container, the usage status such as the number of times the content is permitted to be further reproduced, described in the content usage control status (UCS) information stored in the memory **1834** is checked, the content is used, that is, decryption is performed, within the restriction set therein.

[**0481**] In the content distribution using secure containers, when primary distribution is performed from a service provider to a user device or when secondary distribution (intergeneration distribution or secondary transmission) is performed among a plurality of user devices, user authentication is performed using a person identification certificate (IDC). Furthermore, use of a content is limited within the restriction defined in the "UCP generation management information" and the "UCP allowable number of secondary distributions" included in the sales restriction (UCP) information in the secure container. Furthermore, reception of the content usage charge resulting from primary distribution or secondary distribution (intergeneration distribution or secondary transmission) can be automatically performed in accordance with the reception log generated in accordance with the price information and the sales restriction information described in the secure container. Thus, an additional process for settlement is not necessary.

[**0482**] [7. Link Between Person Identification Certificates (IDC) and Public Key Certificates (PKC)]

[**0483**] Manners of relating person identification certificates (IDCs) to public key certificates (PKC), that is, manners of forming links therebetween are described below.

[**0484**] In many situations, it is useful to manage person identification certificates (IDCs) and public key certificates (PKCs) by relating them with each other. For example, a person identification certificate (IDC) may be linked to a public key certificate of a public key applied to encryption of a template stored in the person identification certificate, or, a link may be formed between a person identification certificate and a public key certificate which are used in person authentication, mutual authentication, and transmission of encrypted data during a process of establishing a connection for data communication with a party such as a particular service provider, so that one certificate can be pointed to by the other certificate.

[**0485**] Links between person identification certificates (IDCs) and public key certificates (PKCS) may be formed not only in a one-to-one fashion in which one person identification certificate (IDC) is linked to one public key certificate (PKC), but also in a one-to-many, many-to-one, or many-to-many fashions. There is a one-to-one correspondence between PKCs and IDCs when an unique person identified by a person identification certificate (IDC) corresponds to an unique public key certificate (PKC). For example, when one device and one user of that device correspond to each other in a one-to-one fashion, a one-to-one link may be formed.

[**0486**] PKCs and IDCs may be linked in a one-to-N ({>=} 2) fashion, when, for example, a plurality persons identified by a plurality of person identification certificates (IDCs) do not correspond to one public key certificate, that is, one

device is shared by a plurality of users. PKCs and IDCs may be linked in a one-to-M ({>=} 2) fashion, when, for example, there are a plurality of public key certificates that an unique person identified by a person identification certificate (IDC) uses or can use. PKCs and IDCs may be linked in a M-to-N (M, N {>=} 2) fashion, when, for example, there are a plurality of public key certificates that a plurality of persons identified by a plurality of person identification certificates (IDCs) use or can use and a device is shared by the plurality of persons.

[0487] Furthermore, person identification certificates (IDCs) and public key certificates (PKCs) may be linked in a one-way fashion (one direction link, directional link) in which only one type of certificates can be pointed to by the other type of certificates or in a two-way fashion in which any type of certificates can be pointed to by the other type of certificates.

[0488] Specific examples of manners of forming links between person identification certificates (IDCS) and public key certificates (PKCs) are described below with reference to **FIGS. 47A and 47B** and **FIGS. 48A and 48B** for the respective cases of one-to-one, one-to-many, many-to-one, and many-to-many links. In any example described below, it is assumed that person identification certificates (IDCs) are issued by a person identification certificate authority (IDA) and a signature of the person identification certificate authority (IDA) is written therein, and it is also assumed that public key certificates (PKCs) are issued by a certificate authority (CA) and a signature of the certificate authority (CA) is written therein.

[0489] In any case, links can be formed in one of various manners described below.

[0490] (1) A PKC identification number is embedded in an IDC

[0491] (one-way link from the IDC to the PKC)

[0492] (2) An IDC identification number is embedded in a PKC

[0493] (one-way link from the PKC to the IDC)

[0494] (3) A link structure ID is embedded in an IDC and a PKC.

[0495] The link structure is identified by a link structure ID, and the link structure has an IDC identification number and a PKC identification number of the linked IDC and PKC.

[0496] (two-way link between the IDC and the PKC)

[0497] (4) A pair of a PKC identification number and an IDC identification number is described in the outside of certificates.

[0498] (one-way link from the IDC to the PKC)

[0499] (5) A pair of a PKC identification number and an IDC identification number is described in the outside of certificates.

[0500] (one-way link from the PKC to the IDC)

[0501] (6) A pair of a PKC identification number and an IDC identification number is described in the outside of certificates.

[0502] (two-way link between the PKC and the IDC)

[0503] (7) A PKC is stored in an IDC

[0504] (one-way link from the IDC to the PKC)

[0505] (8) An IDC is stored in a PKC

[0506] (one-way link from the PKC to the IDC)

[0507] (9) A link information inquiry number or inquiry information is stored in each certificate

[0508] (one-way link from one of the PKC and the IDC to the other or two-way link between them)

[0509] As described above, link information may be stored in such a manner that an identification number of a linked certificate is stored (embedded) in a person identification certificate (IDC) itself or a public key certificate (PKC) itself as in (1) and (2), or in such a manner that a link structure indicating a correspondence between identification numbers of linked certificates is created and an identifier (ID) of the link structure is described in a person identification certificate (IDC) or a public key certificate (PKC), that is, the link structure identifier serving as link identification data and identifiers of linked public key certificate identifiers and person identification certificates are stored as in (3). Furthermore, as in (4), (5), and (6), link information indicating links between person identification certificates (IDCs) and public key certificates (PKCS) is collected and managed in the outside of the certificates in an integral fashion by an agency or an organization, for example, by a link information management center or the like located on a network, and ink information is extracted as required. Specific examples of the manners of forming links are described below.

[0510] (PKC is Stored in IDC)

[0511] As described earlier, one manner of storing template information identifying a person in a person identification certificate (IDC) is to encrypt the template using a public key and store the encrypted template in the person identification certificate (IDC). A public key certificate (PKC) which is generated in correspondence with the public key used to encrypt the template is set as a linked public key certificate (PKC) of the person identification certificate (IDC), and this linked public key certificate (PKC) is stored in the person identification certificate (IDC). **FIG. 49A** illustrates a manner in which a linked public key certificate (PKC) is stored in a person identification certificate (IDC).

[0512] As shown in **FIG. 49**A, the encrypted template and the public key certificate (PKC) of the public key applied to encryption of the template are stored in the person identification certificate (IDC). As described earlier, the public key applied to the encryption of the template is one of a public key of a user or a user device, a public key of service provider (SP), and a public key of a person identification certificate authority (IDA), and the public key certificate (PKC) stored in the person identification certificate (IDC) is that of the public key employed to encrypt the template. By forming the link in the above-described manner, the person identification certificate (IDC) and the public key certificate (PKC) of the public key used to encrypt the template are combined together, that is two types of certificates are combined together in an inseparable fashion. When certifi-

cates are linked in this manner, it is desirable that the expiration dates of the certificates be set such that the expiration date of the IDC {<=} the expiration date of the PKC. That is, it is desirable that the expiration dates be set such that the PKC stored in the IDC becomes valid during the entire period in which the IDC is valid.

[0513] (IDC is Stored in PKC)

[0514] **FIG. 49B** illustrates a manner in which a linked person identification certificate (IDC) of a public key certificate (PKC) is stored in the public key certificate (PKC) which is generated in correspondence with a public key employed to encrypt a template.

[0515] As shown in **FIG. 49**B, the linked person identification certificate (IDC) including template information encrypted with the public key corresponding to the public key certificate (PKC) is stored in the public key certificate (PKC). As described earlier, the public key applied to the encryption of the template is one of a public key of a user or a user device, a public key of a service provider (SP), and a public key of a person identification certificate authority (IDA), and the public key certificate (PKC) in which the person identification certificate (IDC) is stored is that of the public key employed to encrypt the template. By forming the link in the above-described manner, the person identification certificate (IDC) and the public key certificate (PKC) of the public key used to encrypt the template are combined together, that is, two types of certificates are combined together in an inseparable fashion. Note that the person identification certificate (IDC) itself exists independently. When certificates are linked in this manner, it is desirable that the expiration dates of the certificates be set such that the expiration date of the PKC {<=} the expiration date of the IDC. That is, it is desirable that the expiration dates be set such that the IDC stored in the PKC becomes valid during the entire period in which the PKC is valid.

[0516] (Identifier of a Linked Certificate is Stored in a Certificate)

[0517] A manner is described in which an identifier of a certificate such as an unique identification number assigned to that certificate is stored in a certificate to be linked to the former certificate.

[0518] **FIG. 50A** shows a manner in which an identification number of a public key certificate (PKC) is stored in a person identification certificate (IDC), and **FIG. 50B** shows a manner in which an identification number of a person identification certificate (IDC) is stored in a public key certificate (PKC).

[0519] In the example shown in **FIG. 50A** in which the identification number of the public key certificate (PKC) is stored in the person identification certificate (IDC), the public key certificate (PKC) is that corresponding to a public key used to encrypt a template stored in the person identification certificate (IDC), as in the previous example. In this case, it is required that the public key certificate (PKC) should have been issued before the person identification certificate (IDC) was issued. Because it is meaningless to store link information of a public key certificate (PKC) which has expired, it is desirable that the expiration dates be set such that the expiration date of the IDC {<=} the expiration date of the PKC. This link information storage manner is employed, for example, when it is not necessary to store a PKC in an IDC and when it is not desirable to distribute the PKC together with the IDC.

[0520] In the example shown in **FIG. 50B** in which an identification number of a person identification certificate (IDC) is stored in a public key certificate (PKC), not only an identifier of a public key certificate (PKC) corresponding to a public key employed to encrypt a template stored in the person identification certificate (IDC) but also an identifier of a public key certificate (PKC) having some relationship with the person identification certificate (IDC) may also be stored. It is possible to relate a plurality of person identification certificates (IDCs) to a single person identification certificate (IDC). The expiration dates of the IDC and the PKC are not influenced by the validity of the respective certificates. However, only for the certificate of the public key used to encrypt the temple of the IDC, the expiration date should be such as IDC {<=} PKC.

[0521] This link information storage manner may be employed, for example, when after performing user authentication on the basis of a person identification certificate (IDC) in response to a request for access to a device, a plurality of linked public key certificates (PKCs) are used because a public key pair is necessary for each service.

[0522] (Group Information is Managed Separately from PKC and IDC)

[0523] Now, a manner is described in which link management data or group information (link information) indicating a link between a person identification certificate (IDC) and a public key certificate (PKC) is formed separately from both the person identification certificate (IDC) and the public key certificate (PKC), and information which makes it possible to access the link management data is stored in the IDC and the PKC.

[0524] **FIGS. 51A and 51B** and **FIGS. 52A and 52B** show examples of manners of managing links using link management data. In the example shown in **FIG. 51**A, group information (link information) is created and maintained which includes the identifiers (numbers) of a person identification certificate (IDC) and a public key certificate (PKC) and also includes the validity periods of the respective certificates. This method has the feature that the registering/issuing timing of the respective certificates can be independent of each other. Another feature is that a record indicating a relationship between certificates can be generated and managed at a location where the record is required without imposing an influence upon any certificate. It is desirable that the validity period of the group information be set to be equal to the shortest validity period of those of the certificates related to each other. This method may be advantageously employed to mange link information, for example, when user authentication for a plurality of services is performed using one IDC and when different public key pairs are necessary for the respective services.

[0525] In the example shown in **FIG. 51**B, group information (link information) is created and maintained which includes the identifiers (numbers) of a person identification certificate (IDC) and a public key certificate (PKC) and also includes the validity periods of the respective certificates, wherein a group information serial number serving as an identifier of group information is stored in each certificate. The serial number of the group information is identification

data uniquely assigned to each group information by a subject which manages the group information. When a PKC and an IDC linked to each other are issued, data indicating the serial number of the corresponding group information is stored as internal data in each certificate. This method has the feature that addition, change, and deletion of link information described in the group information is possible without causing an influence upon the certificates. This method may be advantageously employed to manage, using group information, the IDCs and PKCs of users to whom services are provided, when it is required that a service provider manage the IDC, PKC, and information related to services.

[0526] In the example shown in **FIG. 52**A, group information serial number serving as an identifier of group information defined as primary information is stored in a person identification certificate (IDC) and a public key certificate (PKC). Furthermore, related information is created as secondary information such that the secondary information can be accessed from the primary information. Accessing to the primary information from the secondary information may also be possible if necessary. Plural pieces of secondary information may be related to primary information and may be managed separately. When a PKC and an IDC are requested to be registered or issued, the serial number of the linked group information is requested to be stored in the PKC and the IDC. Addition, change, deletion of related information does not have an influence upon the certificates.

[0527] In the example shown in **FIG. 52**B, group information (link information) is created and maintained as primary information which includes the identifiers (numbers) of a person identification certificate (IDC) and a public key certificate (PKC), and related information is linked as secondary information such that the secondary information can be accessed from the primary information. The link may also be formed, if necessary, such that accessing to the primary information from the secondary information may also be possible.

[0528] In the case where related information is stored and managed at a plurality of different locations, secondary information identification data and index information are described in primary information so that information can be used and managed flexibly. For example, various service providers (SPs) may be subjects which manage primary information or secondary information, and the respective service providers (SPs) may access person identification certificates (IDCs) and public key certificates (PKCs) of users to which services are to be provided by using the management information as customer information.

[0529] As described above, in various aspects, a person identification certificate (IDC) may be linked to a public key certificate of a public key applied to encryption of a template stored in the person identification certificate (IDC), or a link may be formed between a person identification certificate and a public key certificate which are used in person authentication, mutual authentication, and transmission of encrypted data during a process of establishing a connection for data communication with a party such as a particular service provider, so that one certificate can be easily reached from the other certificate, thereby making it possible to quickly identify a key used in encryption or decryption of a template or to quickly identify data necessary in, for example, mutual authentication on the basis of a public key certificate after person authentication for a service provider on the basis of a person identification certificate.

[0530] [8. Using a Content on the Basis of Person Identification Certificate (IDC) and Public Key Certificate (PKC)]

[0531] A process of performing person authentication on the basis of a person identification certificate (IDC) and receiving (downloading) a content such as music data or image data from a service provider is described below with reference to specific examples.

[0532] As can be understood from the above description, to perform person authentication on the basis of a person identification certificate, the system is required to be capable of comparing sampling information with a template and outputting the comparison result. Herein, a system is described which includes a user device used by a user as a content reproducing device and also includes a mechanism of comparing sampling information with a template, and which also has the capability of downloading a content from a service provider via a network depending upon the comparison result, performing user registration in a service provider, making a contract therewith, and erasing user registration therefrom, and requesting a person identification certificate authority (IDA) to issue a person identification certificate (IDC). The associated processes are also described below.

[0533] **FIG. 53** is a diagram illustrating a configuration of a user device capable of performing person authentication and reproducing a content. A user device **500** includes a contents reproducing mechanism **501**, a contents data storage unit **502**, a user identifying apparatus **503**, a network connection unit **504**, a public key encryption unit **505**, a selection unit **506**, and an input/output unit **507**.

[0534] The contents reproducing mechanism **501** is capable of reproducing a content by reading data from the contents data storage unit. The contents data storage unit **502** serves to download content data via a network and store it therein. The user identifying apparatus **503** serves to input sampling information used to identify an user and convert the input sampling information into digital data and also serves to verify the sampling information by comparing the converted digital data with a template which has already been registered. The network connection unit **504** serves to make a connection to a user device via a network. The public key encryption unit **505** serves to add a signature to specified data, decrypt specified encrypted data, encrypt specified data, create a pair of a public key and a private key, and make a link between an arbitrary public key certificate and certain data. The public key encryption unit **505** is built in the form of a SAM (Secure Application Module). The selection unit **506** serves to select data in a reproducing operation, select a party to which a connection via a network is to be made, and select a content title to be downloaded. The input/output unit **507** serves as a user interface. More specifically, the input/output unit **507** controls a display device and an input device so that specified information is displayed or information input by a user is converted into data having a processable form.

[0535] The public key encryption unit **505** of the user device **500** stores a public key certificate (PKC) and a person

identification certificate (IDC), wherein the public key certificate (PKC) and the person identification certificate (IDC) are described in a mutually linked data format such that either one of the public key certificate (PKC) and the person identification certificate (IDC) can be pointed to by the other one. The specific manner of forming the link has been described above in [Link between Person Identification Certificates (IDC) and Public Key Certificates (PKC)]. A user executes a user authentication process using a person identification certificate (IDC) stored in the public key encryption unit **505**, and the user uses a public key certificate (PKC) in transaction with a service provider.

[**0536**] (Downloading of Content)

[**0537**] A process is described below which is performed by a user device constructed in the above-described manner to download a content such as music data or image data from a service provider and reproduce it, depending upon the result of comparison/verification of sampling information with a template. **FIG. 54** illustrates a flow of data in the contents downloading process, wherein the details of the flow are shown in the **FIGS. 55, 56**, and **57**. The process is described below with reference to these figures. Note that in the following description, the process numbers shown in **FIG. 54** are denoted by (n) and the step numbers in FIGS. **55** to **57** are denoted by (Snnn).

[**0538**] (1) First, to use a device, a user inputs sampling data such as fingerprint information into the device (**S301**). (2) In order to compare the input sampling data with a template of a person identification certificate (IDC) which has already been stored in the SAM, the user identifying apparatus requests the SAM to provide the person identification certificate (IDC) (**S302**).

[**0539**] (3) The SAM retrieves the requested person identification certificate (IDC) on the basis of the link information and returns the retrieved IDC or a template extracted from the IDC to the user identifying apparatus (**S303** to **S305**). (4) The user identifying apparatus compares the sampling data with the template (**S306**). If the comparison result is affirmative, that is, if the user is verified as an authorized user, the user and the network connection unit are informed of the success of the user verification (**S307, S308**). Only when the user verification is affirmative, the network connection unit prepares for connection via the network (**S309**).

[**0540**] (5) The user specifies desired data to be reproduced, via the interface provided by the input/output unit (**S310, S311**). (6) The selection unit converts the command accepted via the interface so as to generate a command for controlling the network connection unit (**S311, S312**) and transmits the control command to the network connection unit (**S313**).

[**0541**] (7) The network connection unit requests the public key encryption unit to provide a public key certificate (PKC) necessary in transaction of content data (**S314** to **S316**).

[**0542**] (8) The public key encryption unit transmits the requested public key certificate (PKC) to the network connection unit (**S317**). In this process, as required, the public key encryption unit retrieves the requested PKC by examining the IDC-PKC link and returns the retrieved PKC to the network connection unit.

[**0543**] (9) The network connection unit accesses a contents data providing server via a local network or the Internet (**S318**). Mutual authentication between the device and the server is performed on the basis of public key certificates, and a shared session key is created thereby establishing a secret communication path (**S319**). In **FIG. 54**, processes (**9-1**) to (**9-8**) are performed when a user communicates with a server in an interactive fashion to receive a service, wherein these processes are performed as many times as required (**S320, S321**). Data is transmitted from the contents providing server to the user via the processes (**9-1**) to (**9-4**), and data is transmitted from the user to the contents providing server via the processes (**9-5**) to (**9-8**). In this data transmission/reception, it is desirable that data be encrypted as required using the session key, signatures be added using the respective private keys, and the signatures be verified using the public key.

[**0544**] (10) After completion of transmission of all data, the network connection unit downloads requested content data from the contents providing server (**S322**). (11) The network connection unit transfers the downloaded content data to the contents data storage unit to store it therein (**S323**), and the session is ended (**S324**).

[**0545**] (12) In the case where reproducing of data is requested by the user, the content data is transferred to the contents reproducing unit (Yes in **S325**). (13) The user executes an operation for reproducing the content using the contents reproducing mechanism (**S326**), and uses the content via the input/output unit.

[**0546**] The flow of downloading and reproducing a content has been described above. Note that the process described above is performed in an easy situation in which a public key certificate (PKC) and a person identification certificate (IDC) are used when a content is downloaded, and these two certificates are stored in the SAM. FIGS. **55** to **57** also show processes which are performed when there is no certificate or when a certificate is not required. The processes performed in such situations are described below.

[**0547**] In **FIG. 56**, steps **S328** to **S332** are performed when a person identification certificate (IDC) corresponding to a user is not found in a user device. In this case, the user device displays a message via an input/output unit to inform the user that the IDC is not found (**S328**) and to request the user to determine whether or not to make a request for issuing an IDC (**S329**). In the case where the user inputs a command indicating that the user does not want the request to be made, the user device informs the user that the downloading has failed (**S332**). On the other hand, if the user inputs a command indicating that the user wants the request for issuing an IDC to be generated, the user device terminates the process of downloading the content and informs the user via the input/output unit that a process of generating a request for issuing an IDC is started (**S330**). Thereafter, the user device executes the process of generating a request for issuing an IDC (**S331**). The details of this process have been described above in [Registration and Change of Template and Person Identification Certificate (IDC)]

[**0548**] In **FIG. 57**, step **S333** and steps following that are performed when the public key certificate (PKC) is not stored in the user device. If acquisition of a public key certificate (PKC) from a certificate authority (CA) located outside is wanted (**S333**), it is determined whether the public

key certificate (PKC) has already been registered (S334). If the registered public key certificate (PKC) is found, the public key certificate (PKC) is acquired from the certificate authority (CA) and stored in the user device (S335).

[0549] If the registered public key certificate (PKC) is not found, it is required to newly issue a public key certificate (PKC). In this case, a pair of a public key and a private key is generated and a request for newly issuing a public key certificate (PKC) is sent to a registration authority (RA), that is, an agency which issues public key certificates (PKCs) (S336). If a public key certificate (PKC) has been newly issued, group information indicating a link to a person identification certificate (IDC) is generated, and the public key certificate is stored (S338). However, the link information may be stored in various manners as described earlier, and thus the above-described process of generating and storing the group information is not necessarily required if the certificate includes link data therein.

[0550] Step S339 and steps following that are performed when issuing of the public key certificate (PKC) is refused. In this case, the user device informs the user via the input/output unit that downloading has failed and the user device terminates the process.

[0551] (User Registration, Erasure of User Registration, and Making Service Contract)

[0552] Now, there is described a process associated with user registration in a service provider which provides various services such as providing of contents, selling of goods, and settlement, erasure of user registration, and making a service contract. Herein, it is assumed that the above process is performed in accordance with user authentication by means of comparison of a template with sampling information, performed by a user identifying apparatus included in a user device shown in **FIG. 53**. **FIG. 58** illustrates a flow of data in user registration, erasure of user registration, and making a service contract, wherein the details of the flow are shown in the **FIGS. 63, 64**, and **65**. The process is described below with reference to these figures. Note that in the following description, the process numbers shown in **FIG. 58** are denoted by (n) and the step numbers in FIGS. **59** to **61** are denoted by (Snnn).

[0553] (1) First, to use a device, a user inputs sampling data such as fingerprint information into the device (S401). (2) In order to compare the input sampling data with a template of a person identification certificate (IDC) which has already been stored in the SAM, the user identifying apparatus requests the SAM to provide the person identification certificate (IDC) (S402).

[0554] (3) The SAM retrieves the requested person identification certificate (IDC) on the basis of the link information and returns the retrieved IDC or a template extracted from the IDC to the user identifying apparatus (S403 to S405). (4) The user identifying apparatus compares the sampling data with the template (S306). If the comparison result is affirmative, that is, if the user is verified as an authorized user, the user and the network connection unit are informed of the success of the user verification (S407, S408). Only when the user verification is affirmative, the network connection unit prepares for connection via the network (S409).

[0555] (5) The user inputs data corresponding to a process to be performed, via the interface provided by the input/output unit. More specifically, in the case of user registration, data indicating a desired site to be registered is input. Data indicating a site the registration of which is to be erased is input in the case of erasure of user registration. In the case of making a contract, data indicating a desired site a contract of which is to be made is input (S410). (6) The selection unit converts the command accepted via the interface so as to generate a command for controlling the network connection unit and transmits the control command to the network connection unit (S411).

[0556] (7) The network connection unit requests the public key encryption unit to provide a public key certificate (PKC) necessary in transaction of content data (S412). (8) The public key encryption unit transmits the requested public key certificate (PKC) to the network connection unit (S413 to S415). In this process, the public key encryption unit retrieves the requested PKC by examining the IDC-PKC link and returns the retrieved PKC to the network connection unit.

[0557] (9) The network connection unit accesses a service registration server or a user registration server via a local network or the Internet (S416). Mutual authentication between the device and the server is performed on the basis of public key certificates, and a shared session key is created thereby establishing a secret communication path (S417). In **FIG. 58**, processes (9-1) to (9-8) are performed when a user communicates with a server in an interactive fashion to receive a service, wherein these processes are performed as many times as required (S418, S419). Data is transmitted from the service registration server or the user registration server to the user via the processes (9-1) to (9-4), and data is transmitted from the user to the service registration server or the user registration server via the processes (9-5) to (9-8). In this data transmission/reception, it is desirable that data be encrypted as required using the session key, signatures be added using the respective private keys, and the signatures be verified using the public key.

[0558] (10) After completion of transmission of all data, the network connection unit downloads necessary data from the service registration server or the user registration server (S420). (11) If the process (user registration, erasure of user registration, making a contract) has been successfully completed, the network connection unit informs the public key encryption unit of the success of the process. Furthermore, if required, necessary information is added to the link information (group information) indicating the link between person identification certificates (IDCs) and the public key certificates (PKCs) (S422, 423). However, the link information may be stored in various manners as described earlier, and thus the above-described process of generating and storing the group information is not necessarily required if the certificate includes link data therein. (12) After completion of the above process, the result of the process is displayed via the input/output unit, and the process is ended (S424, S425).

[0559] The flow of the process has been described above which is performed in connection with the service provider, such as user registration, erasure of user registration, making a service contract, in which user authentication is performed on the basis of a person identification certificate (IDC). Note that the process described above is performed in an easy situation in which a public key certificate (PKC) and a

person identification certificate (IDC) are used, and these two certificates are stored in the SAM. FIGS. **60** to **62** also show processes which are performed when there is no certificate or when a certificate is not required. The processes performed in such situations are described below.

[**0560**] In **FIG. 60**, steps **S426** to **S430** are performed when a person identification certificate (IDC) corresponding to a user is not found in a user device. In this case, the user device displays a message via an input/output unit to inform a user that the IDC is not found (**S426**) and to request the user to determine whether or not to make a request for issuing an IDC (**S427**). In the case where the user inputs a command indicating that the user does not want the request to be made, the user device informs the user that the process has failed (**S430**). On the other hand, if the user inputs a command indicating that the user wants the request for issuing an IDC to be generated, the user device terminates the process of downloading the content and informs the user via the input/output unit that a process of generating a request for issuing an IDC is started (**S428**). Thereafter, the user device executes the process of generating a request for issuing an IDC (**S429**). The details of this process have been described above in [Registration and Change of Template and Person Identification Certificate (IDC)].

[**0561**] In **FIG. 61**, step **S431** and steps following that are performed when the public key certificate (PKC) is not stored in the user device. If acquisition of a public key certificate (PKC) from a certificate authority (CA) located outside is wanted (**S431**), it is determined whether the public key certificate (PKC) has already been registered (**S432**). If the registered public key certificate (PKC) is found, the public key certificate (PKC) is acquired from the certificate authority (CA) and stored in the user device (**S443**).

[**0562**] If the registered public key certificate (PKC) is not found, it is required to newly issue a public key certificate (PKC). In this case, a pair of a public key and a private key is generated and a request for newly issuing a public key certificate (PKC) is sent to a registration authority (RA), that is, an agency which issues public key certificates (PKCs) (**S434**). If a public key certificate (PKC) has been newly issued, group information indicating a link to a person identification certificate (IDC) is generated, and the public key certificate is stored (**S436**). However, the link information may be stored in various manners as described earlier, and thus the above-described process of generating and storing the group information is not necessarily required if the certificate includes link data therein.

[**0563**] Steps **S437** and **S438** are performed when user registration, erasure of user registration, or making a service contract is refused. In this case, the user device informs the user via the input/output unit that the process has failed and the user device terminates the process. Steps **S439** and **S440** are performed when issuing of a new public key certificate (PKC) is refused. In this case, the user device informs the user via the input/output unit that the process has failed and the user device terminates the process.

[**0564**] (Request for a Person Identification Certificate (IDC) to be Stored in a Device and Registration Process)

[**0565**] A process of issuing and registering a person identification certificate (IDC) which is to be stored in a user device including a user identifying apparatus shown in **FIG. 53** is described below. **FIG. 62** illustrates a flow of data in the process of making a request for a person identification certificate (IDC) to be stored in the user device, wherein the details of the flow are shown in the **FIGS. 63, 64**, and **65**. The process is described below with reference to these figures. Note that in the following description, the process numbers shown in **FIG. 62** are denoted by (n) and the step numbers in FIGS. **63** to **65** are denoted by (Snnn).

[**0566**] (1) First, to use a device, a user inputs sampling data such as fingerprint information into the device (**S501**). (2) In order to compare the input sampling data with a template of a person identification certificate (IDC) which has already been stored in the SAM, the user identifying apparatus requests the SAM to provide the person identification certificate (IDC) (**S502**). Herein, it is assumed that there are n person identification certificates (IDCs) which have been issued to the user device and a process is performed to generate a request for issuing a new person identification certificate (IDC) including a template. Note that n=0 in the case where the user device does not have any person identification certificate (IDC).

[**0567**] (3) The user device sequentially retrieves n person identification certificates (IDCs) which have been already stored, and returns the retrieved IDCs or templates extracted from the IDCs to the user identifying apparatus (**S503** to **S505**). (4) The user identifying apparatus compares the sampling data with the templates (**S506**). If the sampling data matches with a template, and thus if it is determined that the user is an authorized user, the user is informed of the success of the user authentication (**S507, S508**). However, in this specific example, it is assumed that the sampling data does not match with the template of any stored person identification certificate (IDC), and thus a request for newly issuing a person identification certificate (IDC) including template information is generated. That is, in the case where even when the sampling data has been compared with the templates of all stored IDCs, any IDC does not have a template which matches with the sampling data, the process goes to step **S509**.

[**0568**] If a person identification certificate (IDC) including a template which matches the sampling information is not found in the user device, the user device displays a message via an input/output unit to inform a user that the IDC is not found (**S509**) and to request the user to determine whether or not to make a request for issuing an IDC (**S510**). In the case where the user inputs a command indicating that the user does not want the request to be made, the user device informs the user that the process has failed (**S512**). On the other hand, if the user inputs a command indicating that the user wants the request for issuing an IDC to be generated, the user device informs the user via the input/output unit that a process of generating a request for issuing an IDC is started (**S511**).

[**0569**] In **FIG. 64**, step **S513** and the following steps are performed to issue a public key certificate (PKC) used in a process of issuing person identification certificate (IDC).

[**0570**] In step **S513**, it is determined whether a public key certificate (PKC) is necessary in the process of issuing a person identification certificate (IDC). If the PKC is not necessary, the process goes to step **S514** to acquire the identification number of the public key certificate (PKC) from an IDC or a PKC or link information (group informa-

tion) stored in the public key encryption unit of the user device. (9) If the public key certificate (PKC) is found (Yes in **S516**), the public key certificate (PKC) is transferred to the public key encryption unit (**S516**), a preparation for connection with an IDRA (registration authority which issues a person identification certificate (IDC)) (**S517**), and information necessary to issue the person identification certificate (IDC) is input (**S518**).

[**0571**] If acquisition of a public key certificate (PKC) from a certificate authority (CA) located outside is wanted (**S520**), it is determined whether the public key certificate (PKC) has already been registered (**S521**). If the registered public key certificate (PKC) is found, the public key certificate (PKC) is acquired from the certificate authority (CA) and stored in the user device (**S522**).

[**0572**] If the registered public key certificate (PKC) is not found, it is required to newly issue a public key certificate (PKC). In this case, a pair of a public key and a private key is generated (**FIG. 62(5)**) and a request for newly issuing a public key certificate (PKC) is sent to a registration authority (RA), that is, an agency which issues public key certificates (PKCs) (**FIG. 62(6), (7)**) (**S336**). In the case where a public key certificate (PKC) has been newly issued (**FIG. 62(8)**) (Yes in **S524**), group information indicating a link to the person identification certificate (IDC) is generated and the public key certificate is stored (**S525**). However, the link information may be stored in various manners as described earlier, and thus the above-described process of generating and storing the group information is not necessarily required if the certificate includes link data therein.

[**0573**] **FIG. 65** shows a process in which a person identification certificate (IDC) is issued by communicating with an IDRA (registration authority which accepts registration of issuing of a person identification certificate (IDC)).

[**0574**] (10) To acquire a person identification certificate (IDC) linked to the public key certificate (PKC), the public key encryption unit of the user device transfers the address of the IDRA and the sampling data (or the user name) to the network connection unit. Herein, it is assumed that the off-line procedure necessary for issue of the person identification certificate (IDC) has already been performed. If information (such as sampling data, PIN, or user name) is further necessary to compare with information (personal information) which has been registered in the off-line procedure and which is used by the IDRA to retrieve the IDC of the user, the information is also transferred at the same time to the network connection unit.

[**0575**] (11) The network connection unit of the user device makes a connection to the IDRA via a local network or the Internet (**S526**). Mutual authentication between the device and the IDRA is performed on the basis of public key certificates, and a shared session key is created thereby establishing a secret communication path (**S527**). The user device transmits necessary information (such as sampling data, PIN, name, address, or telephone number) to the IDRA. An interactive communication process between the user and the IDRA is performed as represented by **(11)-1** to **(11)-8** in **FIG. 62**. **(11)-1** to **(11)-4** are steps performed to transmit data from the IDRA to the user, and **(11)-5** to **(11)-8** are steps performed to transmit data from the user to the IDRA. In this data transmission/reception, it is desirable that data be encrypted as required using the session key, signatures be added using the respective private keys, and the signatures be verified using the public key. In the case where the person identification certificate (IDC) to be issued will include a template encrypted with the public key of the user device, the user device transmits the public key (public key certificate) to the IDRA.

[**0576**] After completion of transmission of all data, the network connection unit downloads necessary data and the result of the IDC issuing request (**S530**). (12) The IDRA verifies the IDC issuing request received from the user device. If it is determined that the request is valid, the IDRA requests an IDCA, which executes an IDC issuing procedure, to issue an IDC. The person identification certificate (IDC) issued by the IDCA is transmitted to the user device via the IDRA.

[**0577**] (13) Upon receiving the person identification certificate (IDC), the user device transmits the person identification certificate (IDC) to the public key encryption unit. (14) The public key encryption unit generates link information (group information) indicating the link between the person identification certificate (IDC) and the public key certificate (PKC) (**S532**) and updates the link information (group information) (**S533**). However, the link information may be stored in various manners as described earlier, and thus the above-described process of generating and storing the group information is not necessarily required if the certificate includes link data therein. (15) After completion of the above process, the result of the IDC issue request process is displayed via the input/output unit, and the process is ended (**S534**, **S535**).

[**0578**] Steps **S536** and **S537** are performed when issuing of the public key certificate (PKC) is refused. In this case, the user device informs the user via the input/output unit that the process has failed and the user device terminates the process. Steps **S538** and **S539** are performed when issuing of a new public key certificate (PKC) is refused. In this case, the user device informs the user via the input/output unit that the process has failed and the user device terminates the process.

[**0579**] [9. One-Time Public Key Certificate (One-Time PKC)]

[**0580**] Now, a process performed by a certificate authority (CA) to issue a public key certificate (PKC) in accordance with user authentication using a template of a person identification certificate authority (IDA) is described. Hereinafter, a public key certificate issued in such a manner is referred to as a one-time PKC. A one-time PKC is issued, for example, when a user wants to perform a transaction such as acquisition of a content from a service provider with which the user has not made a contract, wherein after performing user authentication on the basis of a person identification certificate (IDC) which has already been registered in the person identification certificate authority (IDA), the one-time PKC is issued without performing a rigorous examination of the certificate authority (CA). The one-time PKC is not regarded as an official public key certificate but regarded as valid only in a particular transaction such as a one-time transaction.

[**0581**] **FIG. 66** illustrates a procedure of issuing a one-time PKC. The process proceeds in the order of the numbers shown in **FIG. 66**. **FIG. 67** is a flow chart illustrating the

details of the procedure of issuing a one-time PKC. The process of issuing a one-time PKC is described below with reference to **FIGS. 66 and 67**.

[**0582**] First, an user, who wants to generate a request for issuing a one-time PKC, inputs sampling data such as fingerprint data to an identification request apparatus (**FIG. 67, S201**). The identification request apparatus generates a pair of the public key and the private key of the user who input the sampling data and employing it as a one-time PKC key set (**S202**).

[**0583**] Thereafter, the identification request apparatus performs mutual authentication with a person identification certificate authority (IDA) (**S203**). Provided that the mutual authentication is passed, the identification request apparatus transmits the sampling data, the generated public key, and the user identification data to the person identification certificate authority (IDA). In the transmission of the data, it is desirable that the data be encrypted using the session key, and a signature be attached to the data.

[**0584**] Upon receiving the data from the certificate requesting apparatus, the person identification certificate authority (IDA) extracts a template from the person identification certificate (IDC) which is identified by the user identification data and which has already been registered and compares the received sampling data with the extracted template for verification (**S205**). Thereafter, the person identification certificate authority (IDA) retrieves the user ID from a database (**S206**) and performs mutual authentication between the person identification certificate authority (IDA) and the certificate authority (CA) (**S207**). Provided that the mutual authentication is successfully passed, the person identification certificate authority (IDA) transmits the user ID and the public key to the certificate authority (CA) (**S208**). Also in this data transmission, it is desirable that data be encrypted and a signature be attached to the data.

[**0585**] The certificate authority (CA) generates a public key certificate corresponding to the received public key as a one-time PKC and updates the issue history (**S209, 210**). The certificate authority (CA) transmits the generated one-time PKC to the certificate requesting apparatus via the person identification certificate authority (IDA) (**S211**).

[**0586**] Using the received one-time PKC, for example, the certificate requesting apparatus requests a service provider to provide a service. More specifically, the certificate requesting apparatus adds a signature encrypted with the generated private key to, for example, a content request data or a settlement request data and transmits it together with the public key certificate (one-time PKC) to the service provider.

[**0587**] The service provider extracts the public key certificate (one-time PKC) from the received data, further extracts the public key of the user, and verifies the signature using the public key, thereby verifying the service request (**S215**). If the verification is successfully passed, the service provider provides the requested service (**S215**). Upon receiving the service, the certificate requesting apparatus deletes the public key and the private key generated in the certificate requesting apparatus and also deletes the issued one-time PKC (**S216**). Alternatively, only the public key certificate in the form a one-time PKC may be deleted without deleting the public key and the private key.

[**0588**] The sequence of steps shown in **FIG. 67**, that is, the process from step **S201** in which sampling data is transmitted to step **S216** in which data is deleted, is automatically executed in accordance with a particular processing program which may be provided by the service provider. Thus, the one-time PKC transmitted to the certificate requesting is deleted from the certificate requesting apparatus when the process is completed, thereby ensuring that the one-time PKC is prevented from being used for another transaction. However, it is not necessarily required to delete the one-time PKC, but the one-time PKC may be used repeatedly for particular limited transactions.

[**0589**] As described above, the template serving as user identification data of the user who generates a request for issuing a public key certificate (one-time PKC) is acquired from the person identification certificate and compared with the sampling information to verify the authenticity of the user, and, provided that the user authentication is successfully passed, the public key certificate of the user is issued, thereby making it possible to quickly issue the public key certificate via a simplified issuing procedure.

[**0590**] Furthermore, user authentication is performed at the person identification certificate authority, the certificate authority responsible for issuing public key certificates (one-time PKCs) issues a public key certificate, provided that the user authentication is successfully passed, thereby allowing a reduction in a processing load in terms of the user authentication upon the certificate authority.

[**0591**] Furthermore, because a public key certificate (one-time PKC), which is issued to a user provided that user authentication performed by a person identification certificate authority by comparing user's sampling information with a template stored in a person identification certificate is successfully passed, is deleted when the usage of the public key certificate by an information processing apparatus which has received the public key certificate (one-time PKC) is completed, it is ensured that the public key certificate (one-time PKC) issued via the user authentication performed by the person identification certificate authority can be used only for the particular purpose specified when the one-time PKC is issued.

[**0592**] [10. Verification Certificate]

[**0593**] When a template of a person identification certificate and sampling information match with each other in a verification process, a person identification certificate authority (IDA) certifies that a person who has provided the sampling information is the person corresponding to the person identification certificate. In the examples described above, the verification result is given in the form of a message indicating either OK or NG. Alternatively, the person identification certificate authority (IDA) may issue a verification certificate indicating that user authentication has been successfully passed. The process of issuing the verification certificate is described below.

[**0594**] **FIG. 68** illustrates a first usage manner in which a verification certificate is used. In **FIG. 68**, the process proceeds in the order of numbers from 1 to 10. The further detailed flow is shown in **FIG. 69**. The process is described below with reference to **FIGS. 68 and 69**.

[**0595**] When a user wants to be subjected to person authentication, the user first transmits sampling data to a

person certificate requesting apparatus (**FIG. 69**, **S101**). Herein, the person certificate requesting apparatus is, for example, a user device or a system capable of communicating with a service provider.

[**0596**] Thereafter, the person certificate requesting apparatus performs mutual authentication with a person identification certificate authority (IDA) (**S102**). Provided that the mutual authentication is successfully passed, the user certificate requesting apparatus transmits sampling data and the identifier (ID) of the person certificate requesting apparatus to the person identification certificate authority (IDA) (**S103**). In this data transmission, it is desirable that the data is encrypted using a session key generated in the authentication process or using the public key of the person identification certificate authority (IDA). If the mutual authentication fails, error handling is performed (**S122**), but the following process is not performed.

[**0597**] Thereafter, the person identification certificate authority (IDA) extracts a template of the person identification certificate (IDC) of the user subjected to the person authentication, stored in a database of the person identification certificate authority (IDA) and compares it with the received sampling data. If the verification fails, the following process is not performed.

[**0598**] The person identification certificate authority (IDA) extracts the identifier (ID) of the user subjected to the person authentication from the database of the person identification certificate authority (IDA) (**S105**) and generates a verification certificate on the basis of the ID of the user whose authentication has been successfully passed (**S106**). Furthermore, the person identification certificate authority (IDA) updates the history of issuing verification certificates, that is, writes data indicating the date of issuing the certificate and the validity period thereof into the verification certificate issue history (**S107**). Thereafter, the person identification certificate authority (IDA) issues the verification certificate to the person certificate requesting apparatus.

[**0599**] Furthermore, the process described below is performed when the user requests a service provider to provide a service, using the issued verification certificate. The user, who has received the issued verification certificate, adds a signature to the verification certificate and to an electronic message such as service request data and further attaches the public key certificate thereby generating a service request (**S109**). The generated service request is transmitted to the service provider (**S110**).

[**0600**] The service provider extracts the public key from the received public key certificate and verifies the signature (**S111**). If it is determined that the data has not been tampered with, the service provider provides a service to the user (**S112**). Upon receiving the service, the person certificate requesting apparatus deletes the verification certificate (**S113**).

[**0601**] The sequence of steps shown in **FIG. 69**, that is, the process from step **S101** in which sampling data is transmitted to step **S113** in which the verification certificate is deleted, is automatically executed in accordance with a particular processing program which may be provided by the service provider. Thus, the verification certificate transmitted to the person certificate requesting apparatus is deleted from the person certificate requesting apparatus when the process is completed, thereby ensuring that the certificate is prevented from being used for another purpose. However, it is not necessarily required to delete the certificate, but the certificate may be used repeatedly for particular limited transactions.

[**0602**] **FIG. 70** illustrates a second manner of using a verification certificate. In this example, unlike the example shown in **FIG. 68, a** service provider acquires a verification certificate of a user to whom a service is to be provided.

[**0603**] A user, who wants to request a service provider to provide a service to the user, generates a request data including a service request and sampling data such as fingerprint using a certificate requesting apparatus and writes a signature therein. Thereafter, mutual authentication is performed between the certificate requesting apparatus and the service provider. If it is determined that the mutual authentication has been successfully passed, the service provider transmits the generated request data.

[**0604**] Upon receiving the request data, the service provider verifies the signature to check whether or not the data has been tampered with. If it is determined that the data has not been tampered with, mutual authentication is performed between the person identification certificate authority (IDA) and the service provider. Thereafter, the service provider transmits the sampling data received from the user and the ID of the certificate requesting apparatus together with an attached signature of the service provider

[**0605**] The person identification certificate authority (IDA) verifies the received data to confirm that the data has not been tampered with. Thereafter, the person identification certificate authority (IDA) compares the received sampling data with the template. If it is determined that they match with each other, the person identification certificate authority (IDA) generates a verification certificate. Furthermore, the person identification certificate authority (IDA) generates issue history data and stores it.

[**0606**] The generated verification certificate is transmitted to the service provider. On the basis of the received verification certificate, the service provider determines that the authenticity of the user who has generated the service request has been certified, and the service provider notifies the certificate requesting apparatus and the user that the requested service is to be provided. The service provider deletes the verification certificate, and the process is ended.

[**0607**] **FIG. 71** shows an example of a format of the verification certificate. Respective data items are described below.

[**0608**] Version indicates the version of the verification certificate format.

[**0609**] Serial Number indicates a serial number assigned by a person identification authority (IDA) to a verification certificate.

[**0610**] In Signature algorithm Identifier algorithm parameter, the signature algorithm of the verification certificate and parameters thereof are described. Either the elliptic curve cryptography or the RSA can be used as the signature algorithm, wherein in the case where the elliptic curve cryptography is employed, parameters and the key length are described, while the key length is described in the case where the RSA is employed.

[0611] Issuer is a field in which the issuer of the verification certificate, that is, the name of the person identification certificate authority (IDA) is described in the form of a distinguished name.

[0612] Validity is a field to describe a period during which the certificate is valid, wherein a start date and an expiration date are described.

[0613] Subject is a field in which the name of a subject or a user is described. In this field, more specifically, the ID or the name of the user is described.

[0614] In Subject IDA Info, person identification certificate information of the user, such as the certificate number of the person identification certificate and the unique ID of the person, is described.

[0615] In Subject PKC Infor, the public key certificate information of the person to be certificated, such as the certificate number of the public key certificate of the person to be certificated and the unique ID of the person of the public key certificate of the person to be certificate, is described.

[0616] The digital signature is data which is created by generating a hash value by applying a hash function to all fields of the certificate and then encrypting the resultant hash value using the public key of the person identification certificate authority (IDA).

[0617] As described above, the verification certificate includes the public key certificate information and the person identification certificate information so that links to the public key certificate and the person identification certificate can be formed. The identification data of the person to be certified is also included.

[0618] [11. Downloading of Person Identification Certificate (IDC) and Usage of a Content]

[0619] When a user uses a device in which a person identification certificate (IDC) of that user is not stored, the user can receive a service such as distribution of a content by performing user authentication using a person identification certificate (IDC) which has already been registered in a person identification certificate authority (IDA), as is described below.

[0620] A user, who wants to receive various contents such as music data or image data from a service provider, does not necessarily use a single user terminal (user device) but, in some cases, uses a plurality of devices. For example, the user may use a device installed in his/her home, a device installed in a company, and a device which is opened for use by a plurality of unspecified users.

[0621] To perform person authentication using the above-described person identification certificate (IDC), it is required to access the person identification certificate. For example, if a user device that a user A frequently uses includes a person identification certificate (IDC), person authentication can be performed using the stored IDC. However, it is not realistic that the device installed in the company or the device which is opened for use by a large number of unspecified users include person identification certificates (IDCs) of all possible users. In the device in such a situation, person authentication may be performed using person identification certificates (IDC) which have already been registered in a person identification certificate authority (IDA) to receive a content in accordance with the person authentication, as is described below.

[0622] **FIG. 72** shows a process in which person authentication is performed using a person identification certificate (IDC) which has already been registered in a person identification certificate authority (IDA), and, if the person authentication is successfully passed, a content is distributed to the user. In **FIG. 72**, the process proceeds in the order of numbers from 1 to 11. The further detailed flow is shown in FIGS. **73** to **75**. The process is described below with reference to **FIG. 72** and FIGS. **73** to **75**.

[0623] As shown in **FIG. 72, a** user A executes a process such as reception of a content using a device A of the user A. To this end, the device A includes various certificates which are needed to receive a content. More specifically, a public key certificate (PKC) and a person identification certificate (IDC) of the user A and also a public key certificate (PKC) of the device A are stored in the user device A. The user A can execute a mutual authentication process using various PKCs as required and also can execute a person authentication process using the IDC.

[0624] Herein, it is assumed that the user A receives a service such as distribution of a content using another device. In the specific example shown in **FIG. 72**, the user A uses a device B of a user B to receive a service. A public key certificate (PKC) and a person identification certificate (IDC) of the user B and a public key certificate (PKC) of the device B are stored in the user device B. Although the user B can execute mutual authentication and person authentication using these certificates, the user A, in some cases, cannot execute person authentication or mutual authentication using only the certificates stored in the device B. In such a case, the user A may receive a service of content distribution using the device B, if user authentication on the basis of an IDC and mutual authentication on the basis of a PKC are performed as described below.

[0625] When the user A wants to use the device B, the user A first accesses (activates) the device B (**S801**). To determine whether the access is from a user authorized to access the device B, the device B starts a person authentication process (**S802**). Thus, the user A is requested to input sampling information. In response, the user A inputs sampling information such as a fingerprint and a user ID to the device B (**S803**). The device B retrieves an IDC stored in a storage means in the device B on the basis of the user ID or the sampling information (**S804**). In this specific case, the IDC corresponding to the user A is not stored in the device B, and thus the IDC is not found. In this case, the device B requests a person identification certificate authority (IDA) to transmit the IDC of the user A. In this process, the device B executes mutual authentication with the person identification certificate authority (IDA) and transmits the user ID and the sampling information of the user A to the person identification certificate authority (IDA) after encrypting them using a session key created during the mutual authentication.

[0626] The person identification certificate authority (IDA) retrieves the person identification certificate (IDC) of the user A from a database of the person identification certificate authority (IDA) and transmits the retrieved person identification certificate (IDC) to the device B. The person identification certificate (IDC) includes template informa-

tion which is stored in a form the device B can use. More specifically, for example, the template is encrypted using the public key of the device B. The device B stores the received person n identification certificate (IDC) of the user A in a memory of the device B (S806).

[0627] The device B makes a comparison with the sampling data using the person identification certificate (IDC) of the user A stored in the memory, that is, the device B performs person authentication (S807). If the comparison fails, error handling is performed but the following process is not performed.

[0628] If the person authentication is successfully passed, the device B retrieves a pair of a public key and a private key applicable to the service provided by the service provider (S809). In the data communication with various users for the user authentication or for other purposes, the service provider encrypts the data using a pair of a public key and a private key assigned to each user or each device. In this specific example, a pair of a public key and a private key solely for the user A is not stored in the device B, and thus the result of the decision step S810 becomes negative (No). Thus, the device B creates a new pair of a public key and a private key (S811).

[0629] Thereafter, the device B transmits the generated public key to a certificate authority (CA) to request it to issue a public key certificate, thereby acquiring the public key certificate (PKC) of the user A. The acquired PKC is stored in the device B (S812).

[0630] The device B then forms a link between the person identification certificate (IDC) and the public key certificate (PKC) of the user A. More specifically, for example, the link is formed by creating group information as is described earlier and stores it in the memory. In this process, the link information (group information) is related to service names which are allowed to be used using the IDC and the PKC and registered (S813). That is, to indicate which service provider or which content provider the set of the IDC and the PKC can be used to receive a service from, process identifiers such as provider identifiers or service identifiers are registered together with the link information.

[0631] Thereafter, the device B performs mutual authentication with a service registration server using the public key certificate (PKC) of the user A (S814). The service registration server is a server in which users of one or more service providers (such as a content distribution server) are registered. More specifically, public key certificates (PKCs) of respective users are registered so as to make it possible for a service provider connected to the service registration server to perform, using the registered PKCs, various encryption processes which are needed in, for example, authentication when a service is provided.

[0632] If the mutual authentication with the service registration server is successfully passed, authentication of the user A for the service registration server is performed using the person identification certificate (IDC) of the user A (S816). After completion of these steps, the service registration server registers the public key certificate (PKC) of the user A (S818). Note that, in the above process, the person authentication is executed as required, and it is not necessarily needed. For example, when a content is distributed, person authentication may be performed by a content distribution server.

[0633] The device B receives from the service registration server a message indicating that the public key certificate (PKC) of the user A has been registered, and furthermore the device B receives information about services which are available using the registered public key certificate (PKC) of the user A and also receives PKCs of content distribution servers (S819).

[0634] The following process is performed when a content is received from a content distribution server. In step S820, mutual authentication is performed using the PKC of the content distribution server and the PKC of the user A. If the mutual authentication is successfully passed, distribution of a content is performed (S822). In the above process, in response to receiving a request for a content from the device B, the content distribution server checks whether the PKC used in the mutual authentication performed in response to the request for the content is registered as a PKC for using the content in the service registration server. Only when the PKC is determined to be usable for the content, the distribution of the content is performed. In this specific example, because the public key certificate (PKC) of the user A has already been registered in the service registration server, the request for the content is accepted and the distribution of the content is performed.

[0635] As described above, even when a person identification certificate (IDC) and a public key certificate (PKC) of a user are not stored in a device, a user can receive a service from a service provider by downloading an IDC registered in the person identification certificate authority (IDA) into the device, receiving a public key certificate (PKC) from a certificate authority (CA) using a pair of a public key and a private key generated by the device, performing person authentication on the basis of the IDC, performing mutual authentication on the basis of the PKC, and performing encryption of data.

[0636] The process performed using the person identification certificate (IDC) and the public key certificate (PKC) assigned to a user has been described above. Now, a process performed using a person identification certificate (IDC) assigned to a user and a public key certificate (PKC) assigned to a device is described below.

[0637] **FIG. 76** shows a process in which person authentication is performed using a person identification certificate (IDC) assigned to a user and a public key certificate (PKC) assigned to a device and also using a person identification certificate (IDC) which has already been registered in a person identification certificate authority (IDA), and then a content is distributed to the user using the public key certificate (PKC) assigned to the device. In **FIG. 76**, the process proceeds in the order of numbers from 1 to 6. The further detailed flow is shown in FIGS. **77** to **78**. The process is described below with reference to **FIG. 76** and FIGS. **77** to **78**.

[0638] As shown in **FIG. 76, a** user A usually executes a process such as reception of a content using a device A of the user A. To this end, the device A includes various certificates which are needed to receive a content. More specifically, a public key certificate (PKC) and a person identification certificate (IDC) of the user A and also a public key certificate (PKC) of the device A are stored in the user device A. The user A can execute a mutual authentication process using various PKCs as required and also can execute a person authentication process using the IDC.

[0639] Herein, it is assumed that the user A receives a service such as distribution of a content using another device. In the specific example shown in **FIG. 76**, the user A uses a device B of a user B to receive a service. A person identification certificate (IDC) of the user B and a public key certificate (PKC) of the device B are stored in the user device B. Although the user B can mutual authentication and person authentication using these certificates, the user A cannot execute person authentication using only the certificates stored in the device B. Even in such a case, the user A can receive a content using the device B by performing a process shown in **FIG. 77** and the following figure, in which person authentication is performed using an IDC and mutual authentication is performed using a PKC.

[0640] When the user A wants to use the device B, the user A first accesses (activates) the device B (**S851**). To determine whether the access is from a user authorized to access the device B, the device B starts a person authentication process (**S852**). Thus, the user A is requested to input sampling information. In response, the user A inputs sampling information such as a fingerprint and a user ID to the device B (**S853**). The device B retrieves an IDC stored in the device B on the basis of the user ID or the sampling information (**S854**). In this specific case, the IDC corresponding to the user A is not stored in the device B, and thus the IDC is not found. In this case, the device B requests a person identification certificate authority (IDA) to transmits the IDC of the user A. In this process, the device B executes mutual authentication with the person identification certificate authority (IDA) and transmits the user ID and the sampling information of the user A to the person identification certificate authority (IDA) after encrypting them using a session key created during the mutual authentication.

[0641] The person identification certificate authority (IDA) retrieves the person identification certificate (IDC) of the user A from a database of the person identification certificate authority (IDA) and transmits the retrieved person identification certificate (IDC) to the device B. The person identification certificate (IDC) includes template information which is stored in a form the device B can use. More specifically, for example, the template is encrypted using the public key of the device B. The device B stores the received person n identification certificate (IDC) of the user A in a memory of the device B (**S856**).

[0642] The device B makes a comparison with the sampling data using the person identification certificate (IDC) of the user A stored in the memory, that is, the device B performs person authentication (**S857**). If the verification fails, an error is returned and the following process is not performed.

[0643] If the person authentication is successfully passed, the device B retrieves a pair of a public key and a private key applicable to the service provided by the service provider (**S859**). In the data communication with various users for the user authentication or for other purposes, the service provider encrypts the data using a pair of a public key and a private key assigned to each user or each device. Herein, a pair of a public key and a private key of the device B is usable. The device B performs mutual authentication with a service registration server using the public key certificate (PKC) of the user A (**S814**). The service registration server is a server in which users of one or more service providers (such as a content distribution server) are registered. More specifically, public key certificates (PKCs) of respective users are registered so as to make it possible for a service provider connected to the service registration server to perform, using the registered PKCs, various encryption processes which are needed in, for example, authentication when a service is provided. Herein, it is assumed that the service registration server registers public key certificates (PKCs) of respective devices, or public key certificates (PKCs) of respective devices and person identification certificates (IDCs) of respective users.

[0644] If the mutual authentication with the service registration server is successfully passed, authentication of the user A for the service registration server is performed using the person identification certificate (IDC) of the user A (**S862**). After completion of the above process, the device B receives from the service registration server a message indicating that services are now available and further receives information about what services are available and also receives PKCs of content distribution servers (**S864**).

[0645] The following process is performed when a content is received from a content distribution server. In step **S865**, mutual authentication is performed using the PKC of the content distribution server and the PKC of the device B. If the mutual authentication is successfully passed, distribution of a content is performed (**S867**). In the above process, in response to receiving a request for a content from the device B, the content distribution server checks whether the PKC used in the mutual authentication performed in response to the request for the content is registered as a PKC for using the content in the service registration server. Only when the PKC is determined to be usable for the content, the distribution of the content is performed. In this specific example, because the public key certificate (PKC) of the device B has already been registered in the service registration server, the request for the content is accepted and the distribution of the content is performed.

[0646] As described above, even when a person identification certificate (IDC) and a public key certificate (PKC) of a user is not stored in a device, a user can receive a service from a service provider by downloading an IDC registered in the person identification certificate authority (IDA) into the device, performing person authentication on the basis of the IDC using the public key certificate (PKC) of the device stored in that device, performing mutual authentication on the basis of the PKC, and performing encryption of data.

[0647] [12. Setting the Validity Period of Person Identification Certificate (IDC)]

[0648] As described above, a person identification certificate (IDC) includes template information for identifying a person, such as fingerprint information, a password, or other personal information. Although the template information is encrypted, there is still a non-zero possibility that the template information may be decrypted or tampered with. From this viewpoint, it is undesirable that there are a large number of uncontrolled person identification certificates (IDCs). It is important to control the person identification certificates (IDCs) which are issued by person identification certificate authorities (IDAs) and used by user devices (UDs) or service providers (SPs).

[0649] Now, there is described a method of managing IDCs so as to prevent an IDC and a template from remaining

in a state in which the IDC or the template can be used for a limitless period, by setting the validity information of a person identification certificate (IDC), and more particularly, by setting the period during which the IDC is valid or the maximum number of times the IDC is allowed to be used. By setting the validity period, it becomes possible to examine a user at scheduled intervals, and it also becomes possible to easily check the validity of a user to whom a person identification certificate (IDC) has issued.

[0650] **FIG. 79** illustrates a person identification certificate (IDC) in which validity information (expiration date and the number of times the IDC is allowed to be used) of the person identification certificate (IDC)) and also the expiration date of template information stored in the IDC are set. A person identification certificate authority (IDA) **1001** issues a person identification certificate (IDC) of an user and distributes it to an entity which executes person authentication, such as a service provider (SP)**1002** and a user terminal **1003**. In the service provider (SP) **1002** and the user terminal **1003**, the person identification certificate (IDC) issued by the IDA is stored and is used in person authentication in which sampling information given by a user is compared with information described in the IDC.

[0651] As shown in **FIG. 79**, the person identification certificate (IDC) issued by the person identification certificate authority (IDA) **1001** includes "expiration date or number of times the IDC is allowed to be used"**1004** and "expiration date of template"**1005**, wherein a signature **1006** using a private key of the person identification certificate authority (IDA) is attached to the whole of the IDC. When a service provider **1002** or a user device **1003** receives a person identification certificate (IDC), the service provider **1002** or the user device **1003** verifies the signature **1006** using the public key of the person identification certificate authority (IDA) **1001** to check whether or not the person identification certificate (IDC) has been tampered with.

[0652] The "expiration date or the number of times the IDC is allowed to be used"**1004** stored in the person identification certificate (IDC) is data indicating the validity of the IDC itself. The expiration date or the number of times the IDC is allowed to be used is set by the person identification certificate authority (IDA) **1001** which issues the person identification certificate (IDC) and is stored in the IDC. Even for IDCs in which the template information of the same user is stored, the person identification certificate authority (IDA) **1001** may set different "expiration date or the number of times the IDC is allowed to be used" depending upon service provider or user devices to which the IDCs are provided. When a service provider or a user device performs person authentication using an IDC, the "expiration date or the number of times the IDC is allowed to be used" stored in the person identification certificate (IDC) is verified before making a comparison with sampling information. Only when the expiration date or the number of times the IDC is allowed to be used is met, the comparison is performed.

[0653] The "expiration date of template"**1005** stored in the person identification certificate (IDC) is data indicating the expiration date of the template information stored in the IDC. The "expiration date of template" is set by the person identification certificate authority (IDA) **1001** which issues the person identification certificate (IDC) or by a user himself/herself who provides personal data on the basis of which the template information is generated. In the case where the expiration date of the template information is set by an user, the user sends the expiration date information together with the person identification data to the person identification certificate authority (IDA) **1001**, which in turn sets the expiration date of the template information in accordance with the received expiration date information and stores it in the IDC. When a service provider or a user device performs person authentication using an IDC, the "expiration date or the number of times the IDC is allowed to be used" stored in the person identification certificate (IDC) and also the "expiration date of template" of the template information are verified before comparing sampling information with the template stored in the IDC. Only when the expiration date of the IDC and the expiration date of the template are met, the comparison is performed.

[0654] **FIGS. 80A and 80B** illustrate manners of managing the "expiration date or the number of times the IDC is allowed to be used" and the "expiration date of template" of the template information stored in the person identification certificate (IDC). **FIG. 80A** illustrates an example in which the expiration date of the IDC **1014** and the expiration date of the template **1015** are stored, and **FIG. 80B** illustrates an example in which the number of times the IDC is allowed to be used **1017** and the expiration date of the template **1015** are stored.

[0655] When a service provider or a user device stores into a storage device thereof an IDC, shown in **FIG. 80**A, in which the expiration date of the IDC **1014** and the expiration date of the template **1015** are stored, the IDC is stored after verifying the signature **1016** of the IDC to confirm that the data has not been tampered with. On the other hand, when person authentication is performed using the stored IDC, the expiration date of the IDC **1014** and the expiration date of the template **1015** stored in the IDC are verified before making a comparison with sampling information given by an user. Only in the case where the expiration dates have not been reached, the following process is performed. In the case where either expiration date has been exceeded, error handling is performed and the comparison with the sampling information is not performed.

[0656] When a service provider or a user device stores into a storage device thereof an IDC, shown in **FIG. 80**B, in which the number of times the IDC is allowed to be used **1917** and the expiration date of the template **1015** are stored, the IDC is stored after verifying the signature **1016** of the IDC to confirm that the data has not been tampered with. Furthermore, the SAM information indicating the count of usage of the IDC **1019** set in the IDC is stored in a SAM (Secure Application Module) of the device. In the data stored therein, a signature **1018** is written using a private key of the SAM so as to prevent the data from being tampered with. On the other hand, when person authentication is performed using the stored IDC, the expiration date of template **1015** stored in the IDC and also the SAM information indicating the count of times the IDC is used **1019** stored in the SAM **1020** are verified before making a comparison with sampling information given by an user. Only when the expiration date of the template has not been reached and when the count of usage of the IDC is not equal to zero, the comparison is performed. If the expiration date has been exceeded, or if the count of usage of the IDC is

equal to zero, error handing is performed and the comparison with the sampling information is not performed. In the case where the comparison with the sampling information was performed, the count of usage of the IDC stored in the SAM is reduced (decremented) by one.

[0657] **FIG. 81** illustrates a manner of managing the expiration date of the IDC and the expiration date of the template. First, a person identification certificate authority (IDA) **1001** which issues a person identification certificate (IDC) determines the rule of setting the expiration date of the IDC and the expiration date of the template. A user, who wants a person identification certificate (IDC) to be issued, provides person identification information and personal information needed to issue an IDC to the person identification certificate authority (IDA) **1001**. The person identification certificate authority (IDA) **1001** performs user authentication and verifies the data. If it is determined that the IDC issue request is valid, the person identification certificate authority (IDA) newly issues a person identification certificate (IDC). In the case where the process is performed online, mutual authentication is performed, a signature is added to data to be transmitted, and verification is performed. When a user wants to specify the expiration date of the template, the user sends his/her personal information to the IDA and furthermore informs the IDA of the desired date to be set as the expiration date. The IDA sets the expiration date of the template in the IDC in accordance with the specified date.

[0658] When a service provider **1002** has a transaction with an user, the service provider **1002** requests a person identification certificate authority (IDA) **1001** to issues an IDC for use in user authentication. The person identification certificate authority (IDA) **1001** issues to the service provider **1002** a person identification certificate (IDC) in which the expiration date of the IDC and the expiration date of the template are set. The issued person identification certificate (IDC) includes a signature written using a private key of the person identification certificate authority (IDA) **1001**. When communication is performed between the service provider **1002** and the person identification certificate authority (IDA) **1001**, mutual authentication is performed, a signature is added to data to be transmitted, and verification is performed.

[0659] After verifying the signature using the public key, stored in the service provider **1002**, of the person identification certificate authority (IDA) **1001**, the service provider **1002** stores the IDC in a memory. To authenticate an user, the IDC expiration date and the template expiration date described in the IDC are verified before making a comparison with sampling information. Only when the expiration dates have not been reached, the service provider **1002** accepts sampling information from a user and performs a comparison process. In the example shown in **FIG. 81**, the template information of the person identification certificate (IDC) is encrypted using the public key of the service provider, and thus the template is extracted from the IDC by performing decryption using the private key of the service provider and is used for comparison. If the user authentication is successfully passed, transaction with the user, such as providing of a content, is performed.

[0660] **FIG. 82** illustrates a manner of managing the number of times the IDC is allowed to be used and the template expiration date. First, a person identification certificate authority (IDA) **1001** which issues a person identification certificate (IDC) determines the rule of setting the expiration date of the IDC and the expiration date of the template. A user, who wants issue of a person identification certificate (IDC), provides personal information needed to issue an IDC to the person identification certificate authority (IDA) **1001**. The person identification certificate authority (IDA) **1001** performs user authentication and verifies the data. If it is determined that the IDC issue request is valid, the person identification certificate authority (IDA) newly issues a person identification certificate (IDC). When a user wants to specify the expiration date of the template, the user sends his/her personal information to the IDA and furthermore informs the IDA of the desired date to be set as the expiration date. The IDA sets the expiration date of the template in the IDC in accordance with the specified date.

[0661] When a service provider **1002** has a transaction with an user, the service provider **1002** requests a person identification certificate authority (IDA) **1001** to issues an IDC for use in user authentication. The person identification certificate authority (IDA) **1001** issues to the service provider **1002** a person identification certificate (IDC) in which the number of times the IDC is allowed to be used and the template expiration date are set. The issued person identification certificate (IDC) includes a signature written using a private key of the person identification certificate authority (IDA) **1001**.

[0662] After verifying the signature using the public key, stored in the service provider **1002**, of the person identification certificate authority (IDA) **1001**, the service provider **1002** stores the IDC in a memory. Furthermore, the count of usage of the IDC, set in the IDC, is stored in a SAM (Secure Application Module) of the service provider **1002**. On the other hand, when person authentication is performed using the stored IDC, the template expiration date stored in the IDC is verified and furthermore the count of usage of the IDC stored in the SAM of the service provider **1002** is verified before making a comparison with sampling information given by an user. Only when the expiration date of the template has not been reached and when the count of usage of the IDC is not equal to zero, the comparison is performed. If the expiration date has been exceeded, or if the count of usage of the IDC is equal to zero, error handing is performed and the comparison with the sampling information is not performed. In the case where the comparison with the sampling information was performed, the count of usage of the IDC stored in the SAM is reduced (decremented) by one. In the example shown in **FIG. 82**, in the process of acquiring the person identification certificate (IDC), the user template is encrypted using the public key of the service provider, and thus the template is extracted from the IDC by performing decryption using the private key of the service provider and is used for comparison. If the user authentication is successfully passed, transaction with the user, such as providing of a content, is performed.

[0663] Referring to **FIG. 83**, the process of controlling the usage of an IDC in accordance with the "expiration date or number of times the IDC is allowed to be used" and "expiration date of template" of the person identification certificate (IDC) is described.

[0664] If a service provider or a user device starts to user authentication on the basis of an IDC (**S1001**), a user inputs

or transmits a user ID and sampling data (S1002). The service provider or the user device which performs the person authentication retrieves an IDC on the basis of the user ID and determine whether or not the IDC exists (S1003). If the IDC is not found, the service provider or the user device generates an IDC issue request to a person identification certificate authority (IDA) to acquire the IDC (S1004).

[0665] Thereafter, the "template expiration date" information is extracted from the person identification certificate (IDC) and verifies the template expiration date (S1005). If the expiration date has been reached, the service provider or the user device requests the person identification certificate authority (IDA) to issue an IDC in which a new "template expiration date" is set, thereby acquiring the IDC (S1006).

[0666] The "IDC expiration date" information is then extracted from the person identification certificate (IDC) and verifies the IDC expiration date (S1007). If the expiration date has been reached, the service provider or the user device requests the person identification certificate authority (IDA) to issue an IDC in which a new "IDC expiration date" is set, thereby acquiring the IDC (S1008).

[0667] Thereafter, it is determined whether the "number of times the IDC is allowed to be used" is set in the person identification certificate (IDC) (S1009). If it is set, the count of IDC usage stored in the SAM of the service provider or the user device is read, and it is determined whether the count of IDC usage is equal to zero (S1010). If the count of IDC usage is equal to zero, the service provider or the user device requests the person identification certificate authority (IDA) to issue an IDC in which a new "count of IDC usage" is set, thereby acquiring the IDC (S1011). After acquiring the IDC, the count of IDC usage described in the newly issues IDC is set in the SAM (S1012).

[0668] Thereafter, a template is extracted from the IDC and compared with sampling information given by the user (S1014). After completion of the comparison, if the number of times the IDC is allowed to be used is set in the IDC (Yes in S1015), the count of IDC usage stored in the DAM is decremented by one (S1016). If the count of IDC usage becomes equal to zero (Yes in S1017), the IDC is deleted from the SAM (S1018), and the process is performed depending upon the comparison result (S1019).

[0669] Referring to **FIG. 84**, there is provided a process which is performed to update a person identification certificate (IDC) when a person identification certificate (IDC) is used if it turns out that the "IDC expiration date" has been reached.

[0670] Herein, it is assumed that a person identification certificate (IDC) of a user has been created by a person identification certificate authority (IDA) **1001** and has been transmitted, in response to a request from a service provider **1002**, from the person identification certificate authority (IDA) **1001** to the service provider **1002** and stored in a storage means of the service provider **1002**. The "IDC expiration date" is defined in the person identification certificate (IDC).

[0671] When user authentication is performed before starting a transaction with an user, the service provider **1002** reads the IDC and checks the "IDC expiration date" described in the IDC. If it is detected that the "IDC expiration date" has been reached, the service provider **1002** requests the person identification certificate authority (IDA) **1001** to issue a new IDC. In this case, the service provider **1002** transmits the user ID corresponding to the IDC to be updated to the person identification certificate authority (IDA) **1001**. In the data communication, mutual authentication, addition of a signature, and verification are performed.

[0672] In accordance with the user ID, the person identification certificate authority (IDA) **1001** creates a person identification certificate (IDC) in which a new expiration date is set using the user template information which has already been stored. The created person identification certificate (IDC) is transmitted to the service provider **1002**. The service provider stores the updated IDC in the storage means of the service provider, extracts a template from the updated IDC, decrypts the template, and compares the template with sampling information.

[0673] In a similar manner to the above-described process of updating the IDC expiration date, it is possible to update the number of times the IDC is allowed to be used, and it is also possible to update the template expiration date set by the person identification certificate authority (IDA) when the expiration data has been reached.

[0674] Referring to **FIG. 85**, there is described a process which is performed to update a person identification certificate (IDC) when the checking of the expiration date of the person identification certificate (IDC) reveals that the "IDC expiration date" has been reached.

[0675] Herein, it is assumed that a person identification certificate (IDC) of a user has been created by a person identification certificate authority (IDA) **1001** and has been transmitted, in response to a request from a service provider **1002**, from the person identification certificate authority (IDA) **1001** to the service provider **1002** and stored in a storage means of the service provider **1002**. The "IDC expiration date" is defined in the person identification certificate (IDC).

[0676] The service provider **1002** checks, at scheduled intervals, the expiration date of the person identification certificate (IDC) stored in the service provider **1002**. If it is detected, in the checking at scheduled intervals, that the IDC expiration date has been reached, the service provider **1002** requests the person identification certificate authority (IDA) **1001** to issue a new IDC. In this case, the service provider **1002** transmits the user ID corresponding to the IDC to be updated to the person identification certificate authority (IDA) **1001**. In the data communication, mutual authentication, addition of a signature, and verification are performed.

[0677] In accordance with the user ID, the person identification certificate authority (IDA) **1001** creates a person identification certificate (IDC) in which a new expiration date is set using the user template information which has already been stored. The created person identification certificate (IDC) is transmitted to the service provider **1002**. The service provider stores the updated IDC in the storage means of the service provider.

[0678] In a similar manner to the above-described process of updating the IDC expiration date, it is possible to update the number of times the IDC is allowed to be used, and it is also possible to update the template expiration date set by

the person identification certificate authority (IDA) when the expiration data has been reached.

[0679] Now, a process of updating template information is described. Updating of template information may be performed such that the expiration date of the template information which has already been registered in a person identification certificate authority (IDA) **1001** is simply updated, or such that the template information which has already been registered is deleted and then template information is created in accordance with personal information such as fingerprint information which is newly given by an user. In the case where the existing registered template information is used and only the expiration date is simply updated, updating may be performed in a similar manner as in the updating of the IDC expiration date or the number of times the IDC is allowed to be used. In the case where the expiration date of the template information has been set in accordance with the date specified by an user, the person identification certificate authority (IDA) **1001** may create a person identification certificate (IDC) in which the template expiration date is reset with the approval of the user.

[0680] However, in the case where the existing registered template information is deleted and template information is newly created in accordance with personal information such as fingerprint information which is newly given by an user, it is required to acquire new person identification information from the user. The processes are described below with reference to **FIGS. 86 and 87**.

[0681] **FIG. 86** illustrates a process in which the expiration date of the template information which has already been registered in the person identification certificate authority (IDA) **1001** is checked by the person identification certificate authority (IDA) **1001** and updated if the expiration date has been reached, after informing the user that the expiration date has been reached.

[0682] If the user receives a message indicating that the expiration date of the template information has been reached, the user transmits his/her personal information such as fingerprint data to the person identification certificate authority (IDA) **1001**. Because this process results in re-execution of verification of the identification of the user, it is desirable that the process be performed offline. However, the process may be performed online if it is possible to verify the identification of the user. In this case, mutual authentication between the user device and the person identification certificate authority (IDA) **1001**, addition of a signature to data to be transmitted, and verification are performed.

[0683] The person identification certificate authority (IDA) **1001** verifies the identification of the user and creates a person identification certificate (IDC) in which the person identification data is stored as template information and a new template expiration date is set. The expiration date may be set in accordance with a request from the user. The person identification certificate (IDC) in which the template expiration date has been newly set by the person identification certificate authority (IDA) **1001** is transmitted to a service provider or the like in response to a request, for use in person authentication.

[0684] **FIG. 87** illustrates a process in which template information which has already been registered in a person identification certificate authority (IDA) **1001** is updated in response to an updating request from an user.

[0685] To make a request for updating template information, a user transmits his/her personal information such as fingerprint data to the person identification certificate authority (IDA) **1001**. Because this process results in re-execution of verification of the identification of the user, it is desirable that the process be performed offline. However, the process may be performed online if it is possible to verify the identification of the user. In this case, mutual authentication between the user device and the person identification certificate authority (IDA) **1001**, addition of a signature to data to be transmitted, and verification are performed.

[0686] The person identification certificate authority (IDA) **1001** verifies the identification of the user and creates a person identification certificate (IDC) in which the person identification data is stored as template information and a new template expiration date is set. The expiration date may be set in accordance with a request from the user. Furthermore, as required, for example, in response to a request from an user, the person identification certificate authority (IDA) **1001** may revoke a person identification certificate (IDC) which has already been issued and whose expiration date has not been reached yet. More specifically, revocation of an IDC is performed by issuing an IDC revocation list to a service provider or a user device to which the IDC has been issued. In the IDC revocation list, identification data of revoked IDCs is described. The service provider or the user device, which has received the IDC revocation list, checks whether the IDC revocation list includes an IDC identifier of an IDC which is going to be used in user authentication. If the IDC is included in the IDC revocation list, the IDC is not used. If necessary, the service provider or the user device requests the person identification certificate authority (IDA) to update the IDC and executes user authentication using the updated IDC.

[0687] As described above, when a person authentication execution entity executes person authentication on the basis of a person identification certificate in which a template serving as person identification data is stored, the person authentication execution entity verifies the validity of the person identification certificate on the basis of the certificate expiration date, the number of times the certificate is allowed to be used, or the template expiration date. Only when it is determined that the person identification certificate is valid, person authentication is performed by comparing the template stored in the person identification certificate with sampling information input by an user. This makes it possible for a person identification certificate authority to manage the validity of person identification certificates. The person identification certificate authority may update a person identification certificate or a template in response to a request from an authentication execution entity or a person certified by the person identification certificate. Thus, it becomes possible to update a person identification certificate or a template at an arbitrary desired time. Furthermore, setting the expiration date makes it possible to examine users at scheduled intervals and to easily check the validity of persons certified by person identification certificates (IDCs).

[0688] The present invention has been described in detail above with reference to particular embodiments. It will be

apparent to those skilled in the art that various modifications and substitution to those embodiments may be made in the embodiment chosen for illustration without departing from the spirit and scope of the invention. That is, the embodiments have been described above by way of example and not limitation. The scope of the invention is to be determined solely by the appended claims.

What is claimed is:

1. An information processing apparatus for performing, by a connection to an external server, a process concerning a service provided by the external server,

wherein said information processing apparatus executes person authentication by comparing a template acquired from a person identification certificate storing a template which is person identification data of a user using said information processing apparatus with sampling information input by the user, and performs connection to said external server provided that said person authentication is successfully passed.

2. An information processing apparatus according to claim 1, wherein said information processing apparatus stores a person identification certificate in a memory provided in said information processing apparatus.

3. An information processing apparatus according to claim 1, wherein said information processing apparatus holds link information in which a person identification certificate and a public key certificate applied during a process of establishing a connection to said external server are related to each other and stores the person identification certificate and the public key certificate in a memory provided in said information processing apparatus, and

wherein said information processing apparatus extracts the public key certificate linked to said person identification certificate on the basis of the link information, provided that personal authentication on the basis of said person identification certificate is successfully passed, and performs mutual authentication between said external server and said information processing apparatus by applying the extracted public key certificate.

4. An information processing apparatus according to claim 1, wherein said information processing apparatus is an apparatus having the function of reproducing contents, said external server is a contents providing server, and said information processing apparatus executes person authentication by comparing the template extracted from said person identification certificate with sampling information input by a user, establishes a connection to the contents providing server providing that said person authentication is successfully passed, and downloads the contents.

5. An information processing apparatus according to claim 1, wherein said external server is one of a user registration server and a service registration server which performs any one of processes of user registration, erasure of user registration, and making a service contract to a service providing entity, and

wherein said information processing apparatus executes person authentication by comparing a template extracted from said person identification certificate with sampling information input by a user, establishes a connection to one of said user registration server and the service registration server provided that said person authentication is successfully passed, and transmits necessary data corresponding to any one of said processes of user registration, erasure of user registration, and making a service contract to said user registration server.

6. An information processing apparatus according to claim 1, wherein said information processing apparatus forms a link in which a person identification certificate and a public key certificate applied during a process of establishing a connection for data communication with a party is related to each other, and stores the link in a storage means thereof.

7. An information processing apparatus according to claim 1, wherein said information processing apparatus downloads a person identification certificate applied to person authentication from a person identification certificate authority which is an entity for issuing a person identification certificate and stores the downloaded person identification certificate in a storage means thereof, and

wherein, in a process of downloading said person identification certificate, said information processing apparatus performs mutual authentication between said information processing apparatus and said person identification certificate authority, and downloads the person identification certificate from said person identification certificate authority provided that said mutual authentication is successfully completed.

8. An information processing apparatus according to claim 1, wherein said information processing apparatus downloads a person identification certificate applied to person authentication from a person identification certificate authority which is an entity for issuing a person identification certificate and stores the downloaded person identification certificate, and

wherein, when there is a public key certificate applicable to a process relating to application of the person identification certificate acquired by downloading, said information processing apparatus updates link information in which said person identification certificate and said public key certificate are related to each other, and stores said person identification certificate and said public key certificate in a memory provided in said information processing apparatus.

9. An information processing apparatus according to claim 1, wherein said information processing apparatus downloads a public key certificate from a certificate authority which is an entity for issuing a public key certificate and stores the downloaded public key certificate in a storage means thereof, and

wherein, in a process of downloading said public key certificate, said information processing apparatus performs mutual authentication between said information processing apparatus and said certificate authority, and downloads said public key certificate from said certificate authority provided that said mutual authentication is successfully completed.

10. An information processing apparatus according to claim 1, wherein said information processing apparatus downloads a public key certificate from a certificate authority which is an entity for issuing a public key certificate and stores the downloaded public key certificate in a storage means thereof, and

wherein, when there is a person identification certificate applicable to a process relating to application of the public key certificate acquired by downloading, said information processing apparatus updates link information in which said person identification certificate and said public key certificate are related to each other, and stores said person identification certificate and said public key certificate in a memory provided in said information processing apparatus.

11. An information processing apparatus according to claim 1, wherein said information processing apparatus includes an encryption processing unit, and, in data transmission/reception between said information processing apparatus and said external server, performs mutual authentication between said information processing apparatus and said external server and further, a data transmitting end adds a digital data to the transmitted data and a data receiving end verifies the digital signature.

12. An information processing apparatus according to claim 1, wherein said template is composed of any one of biometric information of a person such as fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information; non-biometric information such as a seal, a passport, a driver's license, and a card; any combination of two or more of said biometric information and said non-biometric information; and a combination of any of said information and a password.

13. An information processing method for performing, by a connection to an external server, a process concerning a service provided by the external server, said method comprising the steps of:

executing person authentication by comparing a template acquired from a person identification certificate storing a template which is person identification data of a user using an information processing apparatus with sampling information input by the user; and

performing a connection to said external server provided that said person authentication is successfully passed.

14. An information processing method according to claim 13, further comprising the steps of:

storing a person identification certificate in a memory provided in said information processing apparatus; and

executing a process by reading the stored person identification certificate during executing personal authentication.

15. An information processing method according to claim 13, wherein said information processing apparatus holds link information in which a person identification certificate and a public key certificate applied during a process of establishing a connection to said external server are related to each other and stores the person identification certificate and the public key certificate in a memory provided in said information processing apparatus, and

wherein said information processing apparatus extracts the public key certificate linked to said person identification certificate on the basis of the link information, provided that personal authentication on the basis of said person identification certificate is successfully passed, and performs mutual authentication between said external server and said information processing apparatus by applying the extracted public key certificate.

16. An information processing method according to claim 13, wherein said information processing apparatus is an apparatus having the function of reproducing contents, said external server is a contents providing server, and said information processing apparatus executes person authentication by comparing the template extracted from said person identification certificate with sampling information input by a user, establishes a connection to the contents providing server providing that said person authentication is successfully passed, and downloads the contents.

17. An information processing method according to claim 13, wherein said external server is one of a user registration server and a service registration server which performs any one of processes of user registration, erasure of user registration, and making a service contract to a service providing entity, and

wherein said information processing apparatus executes person authentication by comparing a template extracted from said person identification certificate with sampling information input by a user, establishes a connection to one of said user registration server and the service registration server provided that said person authentication is successfully passed, and transmits necessary data corresponding to any one of said processes of user registration, erasure of user registration, and making a service contract to said user registration server.

18. An information processing method according to claim 13, wherein said information processing apparatus forms a link in which a person identification certificate and a public key certificate applied during a process of establishing a connection for data communication with a party is related to each other, and stores the link in a storage means thereof.

19. An information processing method according to claim 13, further comprising the steps of:

downloading a person identification certificate applied to person authentication from a person identification certificate authority which is an entity for issuing a person identification certificate to store the downloaded person identification certificate in a storage means thereof;

performing, in a process of downloading said person identification certificate, mutual authentication between said information processing apparatus and said person identification certificate authority; and

downloading the person identification certificate from said person identification certificate authority provided that said mutual authentication is successfully completed.

20. An information processing method according to claim 13, further comprising the steps of:

downloading a person identification certificate applied to person authentication from a person identification certificate authority, which is an entity for issuing a person identification certificate, to store the downloaded person identification certificate; and

updating, when there is a public key certificate applicable to a process relating to application of the person identification certificate acquired by downloading, link information, in which said person identification certificate and said public key certificate are related to each other, to store said person identification certificate and

said public key certificate in a memory provided in said information processing apparatus.

21. An information processing apparatus according to claim 13, further comprising the steps of:

downloading a public key certificate from a certificate authority, which is an entity for issuing a public key certificate, to store the downloaded public key certificate in a storage means thereof;

performing, in a process of downloading said public key certificate, mutual authentication between said information processing apparatus and said certificate authority; and

downloading said public key certificate from said certificate authority provided that said mutual authentication is successfully completed.

22. An information processing method according to claim 13, further comprising the steps of:

downloading a public key certificate from a certificate authority, which is an entity for issuing a public key certificate, to store the downloaded public key certificate in a storage means thereof; and

updating, when there is a person identification certificate applicable to a process relating to application of the public key certificate acquired by downloading, link information, in which said person identification certificate and said public key certificate are related to each other, to store said person identification certificate and said public key certificate in a memory provided in said information processing apparatus.

23. An information processing method according to claim 13, wherein, in data transmission/reception between said information processing apparatus and said external server, said information processing apparatus performs mutual authentication between said information processing apparatus and said external server and further, a data transmitting end adds a digital data to the transmitted data and a data receiving end verifies the digital signature.

24. A program providing medium for providing a computer program which executes, on a computer system, information processing for performing, by a connection to an external server, a process concerning a service provided by the external server, said computer program comprising the steps of:

executing person authentication by comparing a template acquired from a person identification certificate storing a template which is person identification data of a user using an information processing apparatus with sampling information input by the user; and

performing a connection to said external server provided that said person authentication is successfully passed.

* * * * *