

Declaration of Rachel J. Watters on Authentication of Publication

I, Rachel J. Watters, am a librarian, and the Head of Resource Sharing for the General Library System, Memorial Library, located at 728 State Street, Madison, Wisconsin, 53706. Part of my job responsibilities include oversight of Wisconsin TechSearch (“WTS”), an interlibrary loan department at the University of Wisconsin-Madison. I have worked as a librarian at the University of Wisconsin library system since 1998, starting as a graduate student employee in the Kurt F. Wendt Engineering Library and WTS, then as a librarian in Interlibrary Loan at Memorial Library. I began professional employment at WTS in 2002 and became WTS Director in 2011. In 2019, I became of Head of Resource Sharing for UW-Madison’s General Library System. I have a master’s degree in Library and Information Studies from the University of Wisconsin-Madison. Through the course of my studies and employment, I have become well informed about the operations of the University of Wisconsin library system, which follows standard library practices.

This Declaration relates to the dates of receipt and availability of the following:

Sanson, L. D. (Ed.) (1999). *33rd Annual 1999 International Carnahan Conference on Security Technology: Proceedings - The Institute of Electrical and Electronics Engineers: October 5-7, 1999, Madrid, Spain. IEEE.*

Standard operating procedures for materials at the University of Wisconsin-Madison Libraries. When a volume was received by the Library, it would be checked

Declaration of Rachel J. Watters on Authentication of Publication

in, added to library holdings records, and made available to readers as soon after its arrival as possible. The procedure normally took a few days or at most 2 to 3 weeks.

Exhibit A to this Declaration is a true and accurate copy of the front cover, front matter, and back cover of the *33rd Annual 1999 International Carnahan Conference on Security Technology: Proceedings - The Institute of Electrical and Electronics Engineers: October 5-7, 1999, Madrid, Spain* (1999) publication, which includes a stamp on the verso page showing that this book is the property of the Kurt F. Wendt Library at the University of Wisconsin-Madison.

Attached as Exhibit B is the cataloging system record of the University of Wisconsin-Madison Libraries for its copy of the *33rd Annual 1999 International Carnahan Conference on Security Technology: Proceedings - The Institute of Electrical and Electronics Engineers: October 5-7, 1999, Madrid, Spain* (1999) publication. As shown in the "Receiving date" field of this Exhibit, the University of Wisconsin-Madison Libraries owned this volume and had it cataloged in the system as of November 9, 1999.

Attached as Exhibit C is a copy of pages 262 to 279 of the *33rd Annual 1999 International Carnahan Conference on Security Technology: Proceedings - The Institute of Electrical and Electronics Engineers: October 5-7, 1999, Madrid, Spain* (1999) publication.

Declaration of Rachel J. Watters on Authentication of Publication

Members of the interested public could locate the *33rd Annual 1999 International Carnahan Conference on Security Technology: Proceedings - The Institute of Electrical and Electronics Engineers: October 5-7, 1999, Madrid, Spain (1999)* publication after it was cataloged by searching the public library catalog or requesting a search through WTS. The search could be done by title, editor, and/or subject key words. Members of the interested public could access the publication by locating it on the library's shelves or requesting it from WTS.

I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Date: April 24, 2024

Memorial Library
728 State Street
Madison, Wisconsin 53706



Rachel J. Watters
Head of Resource Sharing

EXHIBIT A

1999 IEEE INTERNATIONAL CARNAHAN
CONFERENCE ON SECURITY TECHNOLOGY



89066565995



b89066565995a

1999 IEEE INTERNATIONAL CARNAHAN
CONFERENCE ON SECURITY TECHNOLOGY



HV
7936
E7
I571
y:1999

99CB36303

0-7803-5248-3

1999 IEEE INTERNATIONAL CARNAHAN
CONFERENCE ON SECURITY TECHNOLOGY



89066565995



b89066565995a

0-7803-5248-3

Proceedings

THE INSTITUTE OF ELECTRICAL
AND ELECTRONICS ENGINEERS

33rd ANNUAL 1999 International Carnahan Conference on Security Technology

October 5 - 7, 1999

MADRID, SPAIN

EDITOR
LARRY D. SANSON

Sponsored by:

- IEEE Lexington Section, USA
- IEEE Aerospace and Electronic Systems Society, USA
- Chung Shan Institute of Science & Technology, Taiwan, ROC
- National Chiao-Tung University Taiwan, ROC

In Association With:

- Comisaría General de Policía Científica, Ministerio del Interior
- IEEE Spain Section
- COIT Colegio Oficial Ingenieros Telecomunicación
- SSR, Universidad Politécnica de Madrid
- Securitas Seguridad España, S.A.

Additional Records are available from:

IEEE Service Center
445 Hoes Lane
Piscataway, New Jersey 08854

IEEE Catalog Number 99CH36303
Library of Congress Number 79-644630

ISBN (Softbound) 0-7803-5247-5
ISBN (Casebound) 0-7803-5248-3
ISBN (Microfiche) 0-7803-5249-1

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limits of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 29 Congress Street, Salem, MA 01970. Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication permission, write to Director, Publishing Services, IEEE, 345 E. 47th St., New York, NY 10017. All rights reserved. Copyright© 1995 by The Institute of Electrical and Electronics Engineers, Inc. Printed in the U.S.A.

Kurt F. Wendt Library
University of Wisconsin - Madison
215 N. Randall Avenue
Madison, WI 53706-1688

wend
HV
7936
E7
I571
V, 1999

695707

MEMORIAM

**The 1999 IEEE International Carnahan Conference on Security
Technology Proceedings is dedicated in memory of
THOMAS MAXWELL ANDREWS
7 September 1944 - 21 January 1999**



Tom was born in Cairns, Queensland on 7 September 1944. While attending a secondary school Tom joined the Air Force Cadets and from then on he wanted to be a fighter pilot. When this dream did not eventuate he turned his enquiring mind to electronics and engineering. He served the RAAF for 22 years before joining ASIO (Australian Security Intelligence Organisation).

Tom was a member of the Protective Security Group and his expertise was sought from all areas of the security industry. He liaised with a wide range of Commonwealth government agencies and provided technical advice to State government agencies, most notably the prisons. Tom sought and established links with security industries within the United States and United Kingdom. He established a testing program to share results between these areas and reduce duplication.

Tom was the Australian/South Pacific representative and contact for the Institute of Electrical and Electronic Engineers' (IEEE) International Carnahan Conference on Security Technology (ICCST). He organised the 1997 conference in Canberra which everyone said was a huge success. At last year's conference he was presented with the John S. Jackson award for his efforts.

Tom passed away on the 21st of January 1999 after a short courageous battle with cancer. He will be sorely missed by all who knew him.

Gone but not forgotten

Executive Committee Emeritus

In recognition of their past effort and service devoted to the IEEE International Carnahan Committee on Security Technology, this record of the Proceedings is gratefully dedicated to:

Thomas M. Andrews	—	Attorney General's Department
William D. Barkhau	—	Sylvania Electronic Systems
Benjamin Barker	—	U.S. Army Belvoir R&D Command
Cheryl C. Banks	—	University of Kentucky
Richard J. Blackwell	—	Jet Propulsion Laboratory
David K. Blythe	—	University of Kentucky
Albert C. Brooks	—	Inmont Corporation
Ernst Bunge	—	Bundeskriminalamt, Germany
George C. Byrne	—	SRI International
M. Bruce Carpenter	—	General Electric Aerospace
W. Donald Dodd	—	AESS/IEEE
Tandy Y. Haggard	—	IBM Corporation
Kenneth Hopper	—	Bellcore
John S. Jackson	—	University of Kentucky
Walter S. Konar	—	Stanford University
T.G. Krebs	—	South Central Bell
Benjamin Leon	—	University of Kentucky
Ron McGill	—	Lexington Fayette-Urban-Police
Sue McWain	—	University of Kentucky
Sanford A. Mullings	—	Jamaica Constabulary Office
Richard M. Neal	—	Kentucky Utilities Company
Russell E. Puckett	—	University of Kentucky
Alan N. Rapsey	—	United Kingdom Home Office
John A. Russell	—	Union Carbide Corporation
Guy H. Smith	—	Radiation, Inc.
Earl L. Steele	—	University of Kentucky
Ralph J. Summers	—	Sylvania Electronic Systems
Louis L. Taylor	—	Bernard Johnson Engineering
Carmen J. Tona	—	Consultant

Their professional contributions have so greatly advanced the technology of crime countermeasures and the many years of effort committed to the success of these conferences. Emeritus status is granted to the above persons, which provides complimentary registration to all functions of IEEE International Carnahan Conferences on Security Technology.

Committees

ICCST Executive Committee

Alfonso Bilbao, Conference 1999 President, Spain
Pong-Fui Chang, Microelectronics
Technology, Inc., New Zealand
Hsia-Ling Chiang, National Central University
Chung-Li, Taiwan, ROC
Jiro Chiba, Tohoku University, Sendai, Japan
Ron Clifton, International Datacasting, Canada
Nigel Custance, Securities Facilities Executive, UK
Pieter de Bruyne, Consultant, Switzerland
Gene Greneker, Georgia Tech
Research Institute, USA
Michael Jonckheere, Correctional Service, Canada
Henry Kluepfel, Science Applications
International Corp., USA
Richard T. Lazarick, Federal Aviation
Administration, USA
Gerald Levett, G. Levett and Associates, Canada
Dan Pritchard, Sandia National Laboratories, USA
Larry Sanson, Consultant, USA
Clifton L. Smith, Edith Cowan University, Australia
G. Dan Smith, US Department of Energy, USA
Gordon Thomas, Police Scientific
Development Branch, UK
John Veatch, SAIC, Board of Governors,
AESS/IEEE, USA
So-Lin Yen, Ministry of Justice, Taiwan, ROC
Estelle Zannes, University of New Mexico, USA

Organizing Committee

Alfonso Bilbao, Conference 1999 President, Spain
Larry Sanson, Consultant, USA
Gordon Thomas, Police Scientific
Development Branch, UK
Narciso García, SSR, Universidad Politécnica
Madrid, Spain
Magdalena Salazar, IEEE Spanish Section, Spain
Adrián Nogales, Colegio Oficial Ingenieros de
Telecomunicación, Spain
José Miguel Otero, C. G. Policía Científica,
Ministerio del Interior, Spain

International Advisory Committee

Alfonso Bilbao, Conference 1999 President, Spain
Pong-Fui Chang, Microelectronics
Technology, Inc., New Zealand
Hsia-Ling Chiang, National Central University
Chung-Li, Taiwan, ROC
Jiro Chiba, Tohoku University, Sendai, Japan
Ron Clifton, International Datacasting, Canada
Nigel Custance, Securities Facilities Executive, UK
Pieter de Bruyne, Consultant, Switzerland
R. Deng, National University of Singapore,
Singapore
R. Govaerts, Katholieke
Universiteit Leuven, Belgium
Gene Greneker, Georgia Tech
Research Institute, USA
Michael Jonckheere, Correctional Service, Canada
Henry Kluepfel, Science Applications
International Corp., USA
Richard T. Lazarick, Federal Aviation
Administration, USA
Gerald Levett, G. Levett and Associates, Canada
Peter C. K. Liu, Hong Kong Polytechnic, ROC
H. Luck, Duisburg University, Germany
Dan Pritchard, Sandia National Laboratories, USA
Larry Sanson, Consultant, USA
Clifton L. Smith, Edith Cowan University, Australia
G. Dan Smith, US Department of Energy, USA
Gordon Thomas, Police Scientific
Development Branch, UK
John Veatch, SAIC, Board of Governors,
AESS/IEEE, USA
C. W. Wannerskog, AB DETEKTOR, Sweden
So-Lin Yen, Ministry of Justice, Taiwan, ROC
Estelle Zannes, University of New Mexico, USA

Table of Contents

KEYNOTE ADDRESSES

- Problems of Physiognomic Identification with Video Cameras** 21
Dr. Juan López Palafox, Comisaría General de la Policía Científica,
Spain
- The Understanding of Security Technology and Its Applications** 26
Clifton Smith, Edith Cowan University, *Australia*

SESSION I — SENSORS & ALARM ASSESSMENT I

Moderator: Alfonso Bilbao
IEEE ICCST 1999 Chairman

- Design and Implementation of a Non-Threatening Barrier
for Deployment in Special Usage Holding Areas** 38
Nigel Buckley, *Australia*
- Automatic CCTV Surveillance — Towards the VIRTUAL GUARD** 42
Geoff Thiel, *UK*
- New Microwave Sensors for Intrusion Detection Systems** 49
Felix Perez Martínez, Fernando Casanova Galeano, *Spain*
- Intruder Sensor Using Low Probability of Interception SS-FH Signals** 54
Juan Sanmartín-Jara, M. Burgos-García, J. Retamosa-Sánchez, *Spain*
- Multisensorial Modular System of Monitoring and Tracking
with Information Fusion Techniques and Neural Networks** 59
Javier Durán de Jesús, Juan J. Villacorta Calvo, Alberto Izquierdo Fuente,
Spain

SESSION II — POLICE TECHNOLOGY

Moderator: Jose M. Otero
Comisaría General Policía Científica,
Ministerio del Interior, *Spain*

- Neural Networks Applied to Gun and Ammunition
Recognition from Shooting Sounds** 67
Angélica González Arrieta, Luis Alonso Romero, Angel L. Sánchez
Lázaro, Jose M. Del Amo Rodríguez, J. R. García, *Spain*
- Automatic Car Plate Detection and Recognition
through Intelligent Vision Engineering** 71
Luis Salgado, José M. Menéndez, Enrique Rendón, Narciso García,
Spain

The Vocal Passport, A Technique to Outline Profiles of Criminals from Their Voice Recordings	77
Carlos Delgado Romero, <i>Spain</i>	
Moderate Computational Load Watermarking System for Digital Images	80
José M. Martinez, M. Luisa Mora, <i>Spain</i>	

SESSION III — SENSORS & ALARM ASSESSMENT II

Moderator: Gordon Thomas
Police Scientific Development Branch, UK

A New Approach to Prison Control Room Design	85
Alan Lindfield, <i>UK</i>	
Non Destructive Testing of Fence Mounted PIDS	90
Ian J. Wassell, <i>UK</i>	
Solid State Simulation of Movements for the Test of Volumetric Intrusion Detectors	95
Ingolf Williams, Martin Berentsen, Claudia Rexfort, <i>Germany</i>	
Analyses of Performance of Volumetric Intrusion Detection Technologies	101
A. Lester, C. L. Smith, <i>Australia</i>	
User Performance Testing of the Perimetrix® Buried Cable Sensor	112
Mel Maki, Charles Hill, <i>Canada</i>	

SESSION IV — AIRPORT SECURITY

Moderator: John Veatch
SAIC, Executive Committee, AESS/IEEE, USA

Airport Vulnerability Assessment — A Methodology Evaluation	120
Rick Lazarick, <i>USA</i>	
An Airport Vulnerability Assessment Methodology	134
John D. Veatch, Joseph W. James, Terry T. May, Thomas M. Wood, Eric M. Kruse, <i>USA</i>	
Human Factors Considerations for Aviation Security Technologies	152
Eric C. Neiderman, J. L. Fobes, <i>USA</i>	
Evaluation of the FAA's Security Equipment Integration Program	158
Rodger Dickey, Ed Rao, <i>USA</i>	
Advanced Technology Explosives Detection Device Deployment in the FAA's Security Equipment Integrated Program	168
Ed Rao, Keith Goll, <i>USA</i>	

SESSION V — PERSONNEL & MATERIAL ACCESS CONTROL

Moderator: Rick Lazarick
FAA, Airport Security RID AAR-510, USA

Privacy Algorithm for Cylindrical Holographic Weapons Surveillance System	177
Paul E. Keller, Douglas L. McMakin, David M. Sheen, A. David McKinnon, Jay W. Summnet, <i>USA</i>	
Face Identification by Means of a Neural Net Classifier	182
Virginia Espinosa-Duró, Marcos Faúndez-Zanuy, <i>Spain</i>	
Remote Access Control by Means of Speech	187
Carlos Vivaracho, Luis Alonso Romero, Q. Isaac Moro, <i>Spain</i>	
Fully Integrated Digital Imaging in an Access Control and Security System	191
Charles Oram, Felix Collins, Nick Body, <i>New Zealand</i>	
Motorway Surveillance through Stereo Computer Vision	197
Jose M. Menéndez, Luis Salgado, Enrique Rendón, Narciso García, <i>Spain</i>	

SESSION VI — BIOMETRIC IDENTIFICATION I

Moderator: Narciso García
SSR, Universidad Politécnica Madrid, Spain

Biometric Identification System Based in Keyboard Filtering	203
Oscar Coltell, Guillermo Torres, José M. Badía, <i>Spain</i>	
O'Hare International Airport's Air Cargo Security Access System	210
Martha Snyderwine, Dan Murray, <i>USA</i>	
Identification of Individuals Using Fingerprints by Linguistic Descriptions Fuzzy Comparison	227
Angel Luis Puebla Martínez, <i>Spain</i>	
Evaluation of JTC Method Robustness in Security Applications	233
Milos Klíma, <i>Czech Republic</i>	

SESSION VII — BIOMETRIC IDENTIFICATION II

Moderator: Clifton Smith
Edith Cowan University, Australia

Biometric Identification through Speaker Verification over Telephone Lines	238
Joaquín González-Rodríguez, Santiago Cruz-Llanas, Javier Ortega-García, <i>Spain</i>	
Biometrics Verification in a Real Environment	243
Belén Ruiz-Mezcua, Dolores García-Plaza, Cristina Fernandez, Paloma Domingo-García, Fernando Fernandez, <i>Spain</i>	

Modeling Voice Variability through MCE Techniques in Speaker Recognition Systems	247
J. Relaño Gil, C. Martín del Amo, V. Clemente Gómez, L. Hernández Gómez, <i>Spain</i>	

A Dual Speech/Speaker Recognition Using GMM in Speaker Identification and HMM in Keyword Speech Recognition	251
Belén Ruíz, Paloma Domingo, Luis Hernández, <i>Spain</i>	

SESSION VIII — COMMUNICATION & INFORMATION SECURITY I

Moderator: Gerald Levett
G. Levett and Associates, Canada

Auditing Data Warehouse Security	255
Mario Piattini, Jose A. Rodero, <i>Spain</i>	
Digital Image Recording for Court-Related Purposes	262
Harry Rode, Bernd Rieger, <i>Germany</i>	
Security Interface between Metrica and Magerit: Development of Secure Information Systems	280
Arturo Ribagorda, J. M. Sierra, A. Muñoz, <i>Spain</i>	
A Tutorial on Digital Watermarking	286
Juan R. Hernández, Fernando Perez-González, <i>Spain</i>	
Non-Noticeable Information Embedding in Color Images: Marking and Detection	293
Elisa Sayrol, Josep Vidal, Silvia Cabanillas, Sonia Santamaria, <i>Spain</i>	

SESSION IX — COMMUNICATION & INFORMATION SECURITY II

Moderator: Adrián Nogales
Colegio Oficial de Ingenieros de Telecomunicacion, Spain

Solutions for Anonymous Communication on the Internet	298
Joris Claessens, Bart Preneel, Joos Vandewalle, <i>Belgium</i>	
Virus Attack to the PC Bank	304
Fernando de la Puente, Santiago González, Juan D. Sandoval, <i>Spain</i>	
Security Protocols in the Internet New Framework	311
Jose M. Sierra, A. Ribagorda, A. Muñoz, <i>Spain</i> ; N. Jayaram, <i>UK</i>	
A New Public-Key Cryptosystem Family Based on Feedback Shift Registers	318
Raúl Gonzalo Díaz, Miguel Soriano Ibáñez, <i>Spain</i>	
Speech Variability in Automatic Speaker Recognition Systems for Forensic Purposes (Variabilidad del Habla en Sistemas de Reconocimiento Automático de Locutores en Aplicaciones Forenses)	327
J. Ortega-García, S. Cruz-Llanas, J. González-Rodríguez, <i>Spain</i>	

SESSION X — CRYPTOGRAPHY I

Moderator: Estelle Zannes
University of New Mexico, USA

Chaotic Cryptosystems Gonzalo Alvarez, F. Montoya, G. Pastor, M. Romera, <i>Spain</i>	332
A Novel Algorithm for Number Factorization Pedro Zufiria, José A. Alvarez-Cubero, <i>Spain</i>	339
Applied Cryptography in Java Alberto Partida, Diego Andina, <i>Spain</i>	345
Bound for Linear Complexity of Quadratic Functions in F_p Alberto Peinado-Domínguez, F. Montoya Vitini, Jaime Muñoz, <i>Spain</i>	349

SESSION XI — CRYPTOGRAPHY II

Moderator: Pieter de Bruyne
Consultant, Switzerland

A User Authentication Infrastructure for Extranet Applications Javier López, Juan J. Ortega, Antonio Maña, <i>Spain</i>	354
Safe Primes Density and Cryptographic Applications Raúl Durán Díaz, F. Montoya Vitini, J. Muñoz Masqué, <i>Spain</i>	363
Generation of Binary Sequences for Cryptographic Applications Amparo Fuster Sabater, L. J. García-Villalba, <i>Spain</i>	368
Pseudorandom Number Generation Based on Nongroup Cellular Automata Dolores de la Guía Martínez, Alberto Peinado-Domínguez, <i>Spain</i>	370

SESSION XII — SENSORS & ALARM ASSESSMENT III

Moderator: Michael Jonckheere
Correctional Service, Canada

Fence Vibrations Rebecca Gomery, Graham Leach, <i>UK</i>	377
High Discrimination of Nuisance Alarms in a Low Cost Movement Videosensing System for Remote Surveillance of Unattended Sites Rafael Ciria, Jose L. Godoy, Juan Rodrigo, Pilar Cifuentes, Agustin Muñoz-Grandes, <i>Spain</i>	382
Security Vehicles Fleet Management Systems Using GPS Michael A. Molina, <i>Spain</i>	
Campus Security Technology and University Crime: A Comparative Investigation and Analysis Diane Furno-Lamude, Estelle Zannes, <i>USA</i>	391

SESSION XIII — SENSORS & ALARM ASSESSMENT IV

Moderator: Ron Clifton
International Datacasting, Canada

- | | |
|---|------------|
| On the Development of a Digital Video Motion Detection Test Set | 405 |
| Dan A. Pritchard, Jose T. Vigil, <i>USA</i> | |
| Reflections on the Incorporation of Modern Technology
in the Refurbishment of a Victorian Prison | 412 |
| Roger Houchin, <i>UK</i> | |
| Security Communication in Headrace Tunnel
Using Beam Transmission of Laser Lights | 423 |
| Jiro Chiba, Takahira Sato, Norio Sasaki, Katsuhiro Matsuda, <i>Japan</i> | |
| Gryffin TALOS Taut Wire Detection System Real World Experiences | 428 |
| Greg Hellard, <i>Australia</i> | |
| Technology and Security Services | 432 |
| Carlos Martinez, <i>Spain</i> | |

SESSION XIV — COMMUNICATION & INFORMATION SECURITY III

Moderator: Hsia-Liang Chiang
National Central University Chung Li, ROC

- | | |
|---|------------|
| Advanced Method for Improvement of Obscure Video Image | 440 |
| Yuchiro Yamada, <i>Japan</i> | |
| Detecting Security Vulnerabilities in Remote TC/IP Networks:
An Approach Using Security Scanners | 446 |
| Joaquin López Lerida, Silvio Martín Grackzyr, Angel Viña, José Manuel Andujar, <i>Spain</i> | |
| Securing the Itinerary of Mobile Agents through a
Non-Repudiation Protocol | 461 |
| Joan Borrell, Andreu Riera, Sergi Robles, Joan Serra, <i>Spain</i> | |
| On the Design of Campus-Wide Multi-Purpose Smartcard Systems | 465 |
| Chung-Huang Yang, <i>ROC</i> | |

SESSION XV — BIOMETRIC IDENTIFICATION III

Moderator: Fernando Jaureguizar
IEEE Spanish Section

On the Use of Outer Ear Images for Personal Identification in Security Applications	469
Angel Sanchez, Belén Moreno, José F. Vélez, <i>Spain</i>	
An On-Line Signature Verification System Using Multi-Template Matching Approaches	477
Chin-Chuan Han, Pao-Chung Chang, Chao-Chih Hsu, Bor-Shenn Jeng, <i>Taiwan, ROC</i>	
Signature Classification by Hidden Markov Model	481
Miguel A. Ferrer, Jose L. Camino, Carlos M. Travieso, Ciro R. Morales, <i>Spain</i>	
Access Control System with Hand Geometry Verification and Smart Cards	485
Raúl Sanches-Reillo, Ana Gonzalez-Marcos, <i>Spain</i>	

"HISTORY NOTE"

33rd ANNUAL 1999 IEEE INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY

The 1999 IEEE International Carnahan Conference on Security Technology is to be held in Madrid, Spain on October 5-7, 1999 at the facilities of the Spanish Ministerio del Interior in Complejo de Canillas in Madrid. The Conference Chairman is Alfonso Bilbao. His address is:

IEEE INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY

Securitas Seguridad España, S.A.
Alfonso Bilbao Iglesias, Conference President
c/Soto Hidalgo, 1
28042 Madrid, SPAIN

The Conference is directed toward the research and development aspects of electronic security technology. It establishes a forum for the exchange of ideas and dissemination of information on both new and existing technology. Conference participants are stimulated to consider the impact of their work on society.

The IEEE International Carnahan Conference on Security Technology has existed for longer than any other conference, anywhere in the world, on this subject. In addition, it has continuously documented the advances in security technology through its proceedings, published since the 1968 Conference.

The Conference is an interchange of knowledge through the presentation of learned papers. It is where engineers, physicists, scientists and social scientists share with each other the results of their research and product development on crime countermeasures. It has been held each year for the last 32 years.

The Conference derives its name from where it was initially held, the Carnahan House at the University of Kentucky's conference center. This was purchased by the University of Kentucky in 1956 along with the remainder of the estate long known as Coldstream Farm.

The Conference was initiated by Professor Robert Cosgriff, Chairman of the Department of Electrical Engineering at the University of Kentucky. President Johnson had just launched his "war on crime" and Professor Cosgriff felt that a conference on electronic countermeasures would be a worthy contribution to this "war". The first Carnahan Conference, a regional one, was convened in 1967, drawing about a dozen people from Cincinnati, Ohio, Louisville and Lexington.

Three men took the initiative to organize a national conference for the following year: Professor John Jackson, who was editor of the proceedings for 25 years, Lawrence D. Sanson, who was at that time associated with GTE, and Tandy Haggard, who was employed by IBM. Lawrence (Larry) Sanson is the current President of the IEEE Carnahan Conference. The Conference was then sponsored by the College of Engineering, the Lexington Chapter of IEEE, and the Aerospace and Electronic Systems Society section of IEEE.

The Conference then became an annual international event. In addition to Conferences in the USA, the event began to be held abroad every third year. By 1989, six international Conferences had been held: 1973 Edinburgh, Scotland; 1977 Oxford, England; 1980 West Berlin, Germany; 1983 Zurich, Switzerland; 1986 Gothenburg, Sweden; and 1989 Zurich, Switzerland; 1991 Taiwan, R.O.C.; 1995 Sanderstead, England; 1997 Canberra, Australia.

ADOBE – Exhibit 1007, page 20

For many years the Conference utilized the services of the University of Kentucky's Continuing Education Department. In 1986 the Executive Committee of the Conference voted to terminate the arrangement with the University of Kentucky's Department of Electrical Engineering. Additionally, the Georgia Tech Institute of Technology entered the scene as sponsor as did the Aerospace and Electronic Systems Society (AESS) of the IEEE. This was in addition to the Lexington Section sponsorship which had been continuous.

In 1985 the Executive Committee voted to include the word "International" in the name of the Conference and to retain the name "Carnahan". Conferences are held abroad about every other year. In 1991, the Chung Shan Institute of Science and Technology and the National Chiao-Tung University, both of Taipei, Taiwan became permanent sponsors.

The Conference is guided by an "Executive Committee" whose members are from education, industry and government.

Worldwide, there are currently many conferences and workshops devoted to security technology, yet the IEEE International Carnahan Conference on Security Technology continues to be the main international event which brings together those working in this field at the cutting edge of research, development and applications.

Author Index

Alonso Romero, Luis.....	67, 187	Goll, Keith	168
Alvarez, Gonzalo.....	332	Gomery, Rebecca	377
Alvarez-Cubero, José A.	339	González, Santiago.....	304
Andina, Diego	345	González Arrieta, Angélica	67
Andujar, José Manuel	446	Gonzalez-Marcos, Ana	485
		González-Rodríguez, Joaquín	238, 327
		Gonzalo Díaz, Raúl.....	318
Badía, José M.	203		
Berentsen, Martin	95	Han, Chin-Chuan	477
Body, Nick	191	Hellard, Greg.....	428
Borrell, Joan	461	Hernández Gómez, L.....	247
Buckley, Nigel	38	Hernández, Juan R.	286
Burgos-García, M.....	54	Hernández, Luis	251
		Hill, Charles.....	112
Cabanillas, Silvia.....	293	Houchin, Roger	412
Camino, Jose L.	481	Hsu, Chao-Chih.....	477
Casanova Galeano, Fernando	49		
Chang, Pao-Chung	477	Izquierdo Fuente, Alberto	59
Chiba, Jiro.....	423		
Cifuentes, Pilar	382	James, Joseph W.	134
Ciria, Rafael	382	Jayaram, N.	311
Claessens, Joris	298	Jeng, Bor-Shenn	477
Clemente Gómez, V.	247		
Collins, Felix	191	Keller, Paul E.	177
Coltell, Oscar.....	203	Klíma, Milos.....	233
Cruz-Llanas, Santiago	238, 327	Kruse, Eric M.	134
de Jesus, Javier Durán	59	Lazarick, Rick	120
de la Guía Martínez, Dolores	370	Leach, Graham	377
de la Puente, Fernando	304	Lester, A.	101
del Amo Rodríguez, Jose M.	67	Lindfield, Alan	85
del Amo, C. Martín	247	López Lerida, Joaquin	446
Delgado Romero, Carlos.....	77	López, Javier.....	354
Dickey, Rodger	158		
Domingo-García, Paloma	243, 251	Maki, Mel.....	112
Durán Diaz, Raúl.....	363	Maña, Antonio.....	354
		Martín Grackzyr, Silvio	446
Espinosa-Duró, Virginia.....	182	Martinez, Carlos	432
		Martinez, José M.	80
Faúndez-Zanuy, Marcos	182	Matsuda, Katsuhiko	423
Fernandez, Cristina.....	243	May, Terry T.	134
Fernandez, Fernando	243	McKinnon, A. David.....	177
Ferrer, Miguel A.	481	McMakin, Douglas L.	177
Fobes, J. L.	152	Menéndez, Jose M.....	71, 191
Furno-Lamude, Diane	391	Molina, Michael A.....	
Fuster Sabater, Amparo	368	Montoya Vitini, F.....	332, 349, 363
		Mora, M. Luisa	80
García, J. R.	67	Morales, Ciro R.	481
García, Narciso	71, 197	Moreno, Belén.....	469
García-Plaza, Dolores.....	243	Moro, Q. Isaac.....	187
García-Villalba, L. J.	368		
Godoy, Jose L.	382		

Author Index, *continued*

Muñoz Masqué, J.....	349, 363	Snyderwine, Martha	210
Muñoz, A.	280, 311	Soriano Ibáñez, Miguel	318
Muñoz-Grandes, Agustín	382	Summnet, Jay W.	177
Murray, Dan.....	210		
		Thiel, Geoff	42
Neiderman, Eric C.	152	Tichá, Dasa	398
		Torres, Guillermo.....	203
Oram, Charles.....	191	Travieso, Carlos M.	481
Ortega, Juan J.	354		
Ortega-García, Javier	238, 327	Vandewalle, Joos	298
		Veatch, John D.	134
Palafox, Dr. Juan López	21	Vélez, José F.	469
Partida, Alberto	345	Vidal, Josep.....	293
Pastor, G.	332	Vigil, Jose T.	405
Peinado-Domínguez, Alberto	349, 370	Villacorta Calvo, Juan J.	59
Perez Martínez, Félix	49	Viña, Angel	446
Perez-González, Fernando	286	Vivaracho, Carlos	187
Piattini, Mario	255	Volner, Rudolf	398
Preneel, Bart.....	298		
Pritchard, Dan A.....	405	Wassell, Ian J.	90
Puebla Martínez, Angel Luis	227	Williams, Ingolf	95
		Wood, Thomas M.	134
Rao, Ed	158, 168		
Relaño Gil, J.....	247	Yamada, Yuchiro	440
Rendón, Enrique	71, 197	Yang, Chung-Huang	465
Retamosa-Sanchez, J.	54		
Rexfort, Claudia	95	Zannes, Estelle	391
Ribagorda, Arturo	280, 311	Zufiria, Pedro.....	339
Rieger, Bernd	262		
Riera, Andreu	461		
Robles, Sergi.....	461		
Rode, Harry.....	262		
Rodero, Jose A.	255		
Rodrigo, Juan	382		
Romera, M.	332		
Ruíz-Mezcua, Belén	243, 251		
Salgado, Luis	71, 197		
Sanches-Reillo, Raúl	485		
Sánchez Lázaro, Angel L.....	67		
Sanchez, Angel	469		
Sandoval, Juan D.	304		
Sanmartín-Jara, Juan	54		
Santamaria, Sonia	293		
Sasaki, Norio.....	423		
Sato, Takahira	423		
Sayrol, Elisa	293		
Serra, Joan	461		
Sheen, David M.	177		
Sierra, Jose M.	280, 311		
Smith, Clifton.....	26, 101		

EXHIBIT B



Resource description

[Proceedings / International Carnahan Conference on Security Technology. International Carnahan Conference on Security Technology. OES Publications, Lexington, Ky. : Oct. 4-6, 1983- \[1071-6572\]](#)



Holdings [Verona Shelving Facility: Shelving Verona : HV7936 E7 I571 1](#)
 Holdings ID 22812378300002122

[View all holdings](#)
 Barcode 89066565995
 Item ID 23497145480002122
[View all items](#)
 Process type [Loan](#)
 MMS ID 996957073602122
[Browse shelf listing](#)
 Status Item not in place

General

ENUM/CHRON

Notes

History

General Information



Barcode 89066565995
 Copy ID 1
 Material type Book
 Item policy general (book)
 Provenance -
 Is magnetic No
 PO Line
 Issue date -
 Receiving date 11/09/1999
 Expected receiving date -
 Enumeration A 33
 Enumeration B -
 Chronology I 1999
 Chronology J -
 Description 33 1999
 Pages -
 Pieces 1
 Replacement cost -
 Receiving operator import
 Physical condition -
 Process type

Inventory Information



Inventory number	-
Inventory date	-
Inventory price	-

Location Information		▼
Permanent location	Verona Shelving Facility: Shelving Verona (vsf)	
Item call number type	-	
Item call number	-	
Source (Subfield 2)	-	
Storage location ID	-	

Temporary Location Information		▼
Item is in temporary location	No	
Temporary location	-	
Temporary call number type	-	
Temporary call number	-	
Temporary source (Subfield 2)	-	
Temporary item policy	-	
Due back date	-	

Retention Information		▼
Committed to Retain	-	
Retention Reason	-	
Retention Note	-	

EXHIBIT C

Digital Image Recording for Court-Related Purposes

by

Bernd Rieger and Harry Rode

Kriminalistisches Institut, Bundeskriminalamt, D-65173 Wiesbaden, Federal Republic of Germany

Abstract

While the evidentiary value of photographs submitted with original film material (ordinarily a negative or slide) has rarely been contested in the past, it is likely that the susceptibility of digital images to manipulation will lead to increasing doubt with respect to the authenticity of photographic images in the era of digital data processing. Faced with this situation, it is essential that all concerned, and law-enforcement agencies in particular, engage in concerted world-wide efforts to preserve and restore the evidentiary value of photographic images.

This article describes an approach to ensuring the integrity and authenticity of photographic images during the image-recording phase currently favoured by the Bundeskriminalamt. Because the retroactive detection of manipulations on the basis of image content alone is likely to prove quite difficult, this concept presently shows the most promise.

Reflections regarding the basic configuration of a manipulation-proof digital camera capable of meeting the stringent integrity and authenticity requirements imposed for images presented as evidence in court will be discussed. We propose the use of a suitable digital signature, a method that is also used in other cases for the purpose of establishing the binding legal character of a digital expression of intent, as an effective means of protecting digital images against manipulation. Features built into the camera make it relatively easy to record additional characteristic parameters of the image-production process.

These would include the identity of the photographer, global coordinates, date and time, to mention only a few of the most important parameters.

We have reason to hope that camera manufacturers have become aware of the problem in question and will respond with commensurate hardware development and serial production in order to meet the demands of the security market at an acceptable price.

Introduction

Ever since the invention of the camera, photographic documents have traditionally been associated with a high degree of authenticity and have served as convincing evidence in court time and time again. The introduction of digital image processing technology has drastically diminished the traditionally high evidentiary value of photographic images virtually overnight, however. As the quality of digital image-recording devices (scanners, digital cameras, etc.) and output equipment (film and image projectors,

etc.) improves, it is becoming increasingly difficult to detect and show proof of professional image manipulation aided by digital methods. William J. Mitchell has provided an excellent demonstration of what manipulated photos may look like in his article "Digitale Photomanipulation" [WJM94]. The following examples are reprinted with the kind permission of the publisher. Detailed descriptions of the image manipulations can be found in the publication cited above.



Figure 1: This gray-tone reproduction of an older original colour photograph shows the former British Prime Minister Margaret Thatcher in animated conversation with former US President George Bush.



Figure 2b: This manipulated version of Figure 1 evokes an impression of confidential whispering.



Figure 2a: This manipulated version of Figure 1 suggests unpleasant disagreement.

If proof of authenticity has become difficult even for traditional film material, then it is practically impossible for digital images. This is due in part to the easy reproducibility of most digital image-bearing media but also to the fact that, unless specific precautions are taken, digital images have no characteristics that identify them as "originals". In fact, one of the biggest advantages associated with digital data is the ease with which an unlimited number of

identical copies can be made. Other advantages associated with digital images include

- rapid availability without the need for photochemical processing
- world-wide transmission of digital data within minutes or even seconds
- low storage volume
- ease of processing and enhancement
- increasing automation of image retrieval

These properties open up a wide range of new possibilities working with images, of which several are of particular interest to police, especially in cases where images are originally recorded with a digital camera. German police agencies are currently testing first applications in certain areas, e.g. personal surveillance, identification processing and crime scene photography. Economic, organisational, time and productivity considerations clearly suggest that digital recording technology will replace traditional – chemical – photography at least to a certain extent within the next few years. This would also represent a logical step toward digital information processing, which has already been implemented in other areas (such as electronic office communication) at the Bundeskriminalamt.

One significant advantage of digital photography, namely the widespread processing of images using reasonably-priced computers and standard commercial software, will presumably become a major problem in the process. The image manipulation illustrated above can nowadays be accomplished by a practised computer user with only routine computer skills, and – even with the help of modern scientific knowledge – there is no certainty that all such changes could be detected.

Court precedents show that criminal evidence in the form of conventional photographs has been rejected by defence attorneys in only a few well-founded cases on the basis of counsel's doubts about its authenticity. We are concerned that this will change dramatically in the future, in view of the susceptibility of digital images to manipulation. It is entirely probable that defence attorneys in criminal court proceedings will attempt to challenge the integrity and authenticity of potentially incriminating images – motion and still pictures alike.

Thus one essential prerequisite for the recognition of digital photographs as evidence in court remains to be met, namely the possibility of creating a manipulation-proof "original". As the following remarks will show, it should be possible to generate digital "originals" with characteristic qualities that make them at least as resistant to manipulation as conventional photographs (which are also susceptible to manipulation, although with a great expenditure of effort), if not more so.

Requirements for digital photographs in police work

Prior to introduction of digital photo and video technology for police use on broad basis, the following requirements must be imposed upon that technology for the purpose of ensuring the integrity and authenticity of images presented as evidence in court:

- The evidentiary value of digital images for court-related purposes must be enhanced by integrating supplementary information into

the image file. This information should relate specifically to the recording situation, provide reliable identification of the photographer¹ and the camera² and include other relevant data³ as well.

- A solution for manipulation-proof preservation of the original image data together with supplementary information must be found.
- It must be possible to verify image integrity in order to ensure effective protection of digital image data against unauthorised alteration.
- Necessary or useful image-processing techniques (format conversion, scaling, contrast enhancement, compression, etc.) applied must be identifiable.

Simple, published techniques must be available to ensure that the integrity and authenticity of images and supplementary data can be verified by third parties.

Proposed Solution

In 1998, the Bundeskriminalamt commissioned the Erlangen-based Fraunhofer Institute for Integrated Circuits to define the technical and organisational framework conditions for the development of a digital camera that would meet police requirements [Spe98].

In order to ensure the integrity and authenticity of the images produced, a camera of this kind which would be suitable for police work and evidence documentation purposes should provide the following functions:

- generate a digital signature of the image data through a signature component in the camera processor,
- insert a time stamp and possibly record camera parameters,
- possibly insert location data (e.g. using GPS coordinates),
- insert a digital signature of the photographer,

¹ e.g. via registration of his individual smartcard

² e.g. via a CPU serial number

³ e.g. date, time and GPS coordinates for the recording location

- provide physical protection of the image during each stage of the image-production process, from origin in the image sensor to generation of the photographer's signature.

Figure 3 shows the basic conceptual diagram for a digital camera of this kind. The camera processor consists essentially of a high-speed RISC processor, an interface to the CCD chip, serial or parallel ports, an interface to a RAM, a signature chip with a secret key and a data-compression block. Data transfer from the digital camera to an external computer can be effected via a removable memory medium or a suitable parallel or serial port on the camera.

After recording, the processor reads the image data from the CCD sensor and saves these to the RAM. The image file is then compressed (e.g. in the JPEG format), signed and saved to a removable memory medium (floppy disc, semiconductor memory, etc.) or transmitted directly to an external computer.

In order to protect image data against manipulation from the moment they are received in the CCD sensor to generation of the signature, some of the system components, including the CCD sensor, the camera CPU (which also contains a signature chip with the secret key), the RAM, the internal clock, a back-up power supply and the required connector cables must be integrated into a specially protected compartment in the camera housing.

The secure compartment can be protected, for example, by an electrical "protective shield". When this is drilled or severed, a change in potential is triggered and detected by the processor, which then automatically deletes the secret key stored in the signature chip. This ensures that image data cannot be altered without detection prior to application of the signature.

The use of a digital signature for the digital photograph produces the following scenario:

Digital Camera

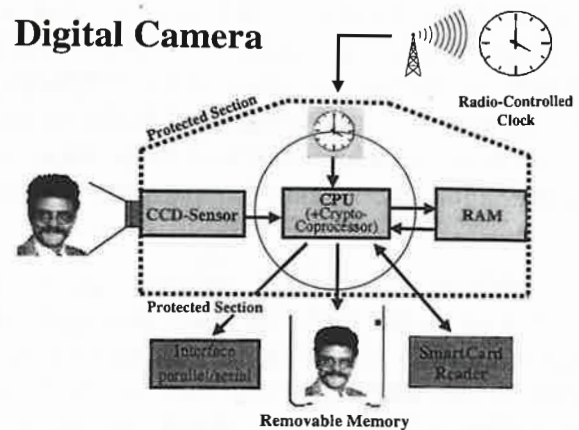


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

The camera is equipped with a SmartCard reader which provides for the use of a signature card (e.g. the new multi-purpose official and installation ID card scheduled for introduction in Germany). Before operating the camera, the photographer inserts his signature card into the built-in card scanner in the camera and activates it by entering his PIN (minimum a six-place code⁴). The card and the camera processor then verify their compatibility. A reciprocal authentication (e.g. via the challenge-and-response method) is possible for certain applications. This requires that the camera processor be equipped with a random-number generator.

The signature chip has the capacity to generate a digital signature. The secret code required for this purpose is contained in the signature chip, along with the signature algorithms and the certifications needed for signature verification. The matching public key for the camera is also recorded in an index on file with the issuing certification service provider.

The image data are read out by the processor, compressed and saved to the RAM. The compressed image data are hashed by the camera processor. The hash total is coded with the secret key of the signature chip and linked together with the image data as the camera signature in the RAM.

⁴ The German Signature Act also expressly provides for the use of equivalent biometric procedures for the identification of the card user.

A highly manipulation-proof time stamp can be obtained using a radio-controlled clock (DCF77; available throughout Central Europe) coupled with an independent reference clock. The reference clock, at the very least, must be integrated into the "secure compartment" of the camera.⁵

The addition of a GPS receiver makes it possible to record both the exact time and the precise location of the camera along with the image data. Although the use of DCF77-compatible clocks is restricted to Central Europe, GPS data are available world-wide.

In principle, all camera parameters, including focus values, aperture settings and exposure times, can be recorded and signed. This also applies to physical data on environmental conditions (e.g. temperature, humidity, etc.)

Before the entire package of image data is saved to the removable camera memory medium, the data are hashed once again by the camera processor, after which the hash value is transmitted to the photographer's signature card in the card reader. There, the hash value (image, camera signature, camera parameters) is encrypted along with the secret key of the photographer's signature card. This encrypted hash value – the actual image signature – is returned to the RAM, where it is linked with the image data already recorded there. Finally, the now complete image data, i.e. –

- the compressed image file,
- the camera signature,
- the recorded camera parameters and
- the photographer's signature,

are saved to the removable memory of the camera. This result might be called a "digital original".

The signature process employed must comply with the requirements of the law and thus with the current state of technology as well. This

means that RSA⁶ (with a key length of 1024 bits) and RIPE MD⁷ or SHA-1⁷ must be used as a hash algorithm (key length 160 bits).

Security Assessment

The process described above is susceptible to the following forms of attack:

1. Loss of the signature card (theft, misappropriation, robbery or misplacement)

If a signature card is lost, stolen, etc., the holder must report the loss immediately to the certification service provider⁸ for entry into an online blocking index. Once the card is blocked, misuse is effectively ruled out. We distinguish between two possible scenarios:

1.1 The unauthorised user knows the PIN

The card remains valid until it is blocked in the blocking index of the certification service provider. Retroactive or post-dated blocking of the card is not possible.

1.2 The unauthorised user does not know the PIN

As the incorrect entry counter restricts the number of incorrect entries to three (or 21 in the case of a master PIN), the probability of guessing a PIN consisting of at least 6 characters is very slight, i.e. about 0.003 ‰ for three attempts and 0.02 ‰ for 21 attempts. The incorrect entry counter cannot be manipulated from the outside.

2. Duplication of a secret camera key or a signature card

The two pairs of keys⁹ (one each for the camera and the signature card) should be

⁵ The company TimeSafe TrustCenter GmbH of Nürnberg holds patents for all time and locating stamping processes involving the comparison and verification of internal and external data.

⁶ See "Asymmetric Encryption Techniques" in Appendix I. Encryption Techniques.

⁷ See Appendix II. Digital Signature.

⁸ See Appendix III. The German Signature Act

⁹ Asymmetric or hybrid encryption processes (see Appendix I. Encryption Techniques) require two keys, one secret and one public.

generated by a certification service provider on the respective cryptochip. The secret key should not be recorded in readable form on the chip. Opportunities for compromise arise when the camera or the signature card is exposed to potential physical manipulation with or without the knowledge of the authorised person. Presently, the hardware and software required for such manipulations is available only in large-scale microchip research institutions. Aside from the technical know-how required, the effort and cost involved in such an operation render the danger of such manipulative attacks virtually negligible at this time.

3. Cracking the codes

The suitability of cryptographic processes used for digital signatures is subject to annual review by a group of leading cryptologists from the fields of science, business and government. Only those processes are assessed as suitable which, given the current state of scientific knowledge and technology, rule out non-detectable forgery of digital signatures or falsification of signed data with virtually total reliability for a period of at least six years.¹⁰ In addition, only processes for which the algorithms have been disclosed are approved for use. A brute-force attack, i.e. an attempt to employ all possible keys, in the case of RSA,⁶ for example, would be so time-consuming that it would take too long (decades or centuries) – judged in terms of the anticipated benefit – to crack a code on the basis of currently available cryptological knowledge.

4. Image reconstruction or reprojection

In the event that a potential attacker gains possession of the camera and the signature card (and knows the PIN), images can be reconstructed or reprojected for the purpose of manipulation. The potential for manipulation in such situations is about the

same as that of conventional photography. Unlike conventional photography, however, our “digital originals” contain additional forensically relevant data – thanks to PIN security, time stamping and, in some cases, location information features – that make the objectives of manipulation virtually impossible to achieve.

5. Alteration of image data

We distinguish between two possible types of cases: unauthorised image manipulation for the purpose of falsifying image contents and necessary or useful image modification intended to produce a more suitable presentation of image content.

5.1 Image manipulation

Because every alteration of image data, regardless of how minor (one bit is enough!), produces a totally different result in the computed check sum (hash total), an integrity test¹¹ will immediately detect any alteration of the data. Thus a non-detectable manipulation of a digital image protected in this way should be impossible.

5.2 Image modification

Necessary or useful modifications of image data (format conversion, scaling, contrast enhancement, compression, restoration, etc.) inevitably produce a negative result in the integrity test. In order to avoid loss of evidentiary value, therefore, modifications of this kind should be undertaken only if the following two conditions are met:

- a. The original image data (positive integrity test) must be preserved in all cases.
- b. The modification must be subject to reconstruction. This means that all steps in the process must be documented precisely. This can be done only if the

¹⁰ Art. 17, Sec.2 of the German Signature Act specifies the Federal Office of Security in Information Processing (BSI) as responsible for verification of the suitability of algorithms and related parameters.

¹¹ The integrity test is described in Appendix II. The Digital Signature

algorithms and parameters selected are exactly known and the outcome of each step in the modification process can be reproduced. The use of image processing programs with unknown functional configurations or non-documentable interaction must be ruled out from the outset.

Under these circumstances, modifications undertaken can be reconstructed at any time on the basis of the original image data.

All in all, the approach described above provides a degree of security with respect to the integrity and authenticity of "digital originals" that should actually exceed that achievable in conventional photographs.

Outlook

Upon completion of the first phase, in which the concept for a digital camera was developed [Spe98], the production of a prototype experimental model of such a camera for laboratory testing was planned for the second phase. The experimental model was to be used to test functional processes, to measure time performance and to test interfaces. The Bundeskriminalamt intended to commission an institute for technical development or an innovative camera manufacturer to perform this work. Although numerous well-known camera manufacturers represented in Germany, many of which operate world-wide, were approached, it has not been possible thus far to find a partner for this project – for which a certain degree of financial commitment will be required – given the budget framework currently available to the Bundeskriminalamt for a project of this kind. Thus our original intention to report on the initial results of the second phase at the 1999 IEEE International

Carnahan Conference on Security Technology cannot be realised. It is hoped that such a report can be presented at a future conference.

Once certified camera hardware and software of the kind described above becomes available, it can be assumed that they will not be used by security agencies and law-enforcement experts alone but will also be employed by professional photographers and semi-professional users. The verifiable integrity and authenticity of digital data can serve to protect photographers' copyrights.

In any case, the widespread availability of these technologies is desirable from the point of view of the police, as mass production will result in a significant reduction in component prices, making it possible to meet the needs of the security market at a reasonable cost. The hope remains that camera manufacturers have become aware of the problem in question and will devote themselves to finding viable solutions if they have not already initiated development efforts in this direction already.

Appendix

I. Encryption Techniques

Experience in recent years has shown that cryptographic methods originally developed to ensure the secrecy of classified documents can also be applied with the aid of certain mathematical operations to a number of other purposes, including the creation of digital signatures.

Protecting the secrecy of stored or transmitted data remains the primary focus of cryptography today. With respect to "secure" data storage or data transmission, however, it is important to take a number of other aspects into account:

- Manipulations of stored information must be detectable.
- The sender of a message must be certain that the message reaches its intended destination without falsification.
- The recipient of a message must be able to verify the authenticity of a message and the correct identity of the sender.

Also of interest are functions comparable to conventional mail with signature or registered mail with return receipt. These include such operations as telebanking from a home computer or e-mail contracts, for which electronic documents may at some time be required as evidence in legal disputes.

In encryption methods currently in use, data are converted with the aid of cryptographic algorithms into a form that can be read only by the person who possess a suitable decoding key.

The encryption process ensures the confidentiality of transmitted data by concealing the content – even when the coded data remain visible as such. Encryption makes secure communication possible even in open networks such as the Internet.

Ordinarily, highly formalised techniques and rules (cryptoalgorithms, encryption routines, etc.) are used in the encryption process. All of

these are based on essentially the same sequential scheme:

- Replace characters (or strings of characters) in a text with other characters (or strings) based upon a key.
- Change the sequence of the encoded characters (may also be based upon a key).
- Repeat the first two steps as often as required.

The real art in developing encryption procedures is to specify the way in which characters are replaced and sequences are changed and the number of times the process is repeated in order to make the job of the cryptanalyst as difficult as possible, on the one hand, and to make the encryption process (implemented on a computer, for example) so fast that the user does not experience undue delays in his work.

Modern cryptographic techniques capable of establishing the authenticity of data were developed as early as twenty years ago. Mathematical functions are the foundation of these digital signatures. The following remarks provide brief, general explanations of these techniques.

SYMMETRIC ENCRYPTION TECHNIQUES

In symmetric encryption techniques, messages are encoded and decoded using the same key. The key must be kept secret by all parties concerned and may be passed between individuals only through secure channels (e.g. personally or via courier).

Symmetric encryption is especially well suited for the conversion of large quantities of data, as the required computations can be performed rapidly by a computer.

One disadvantage of this technique is the complexity involved in key management: Every

sender requires his own secret key for each separate recipient. The potential for compromise of key secrecy increases each time it is passed from one individual to the next. For these reasons, symmetric encryption is not feasible in open networks (e.g. the Internet) involving a large number of participants.

Symmetric Encryption

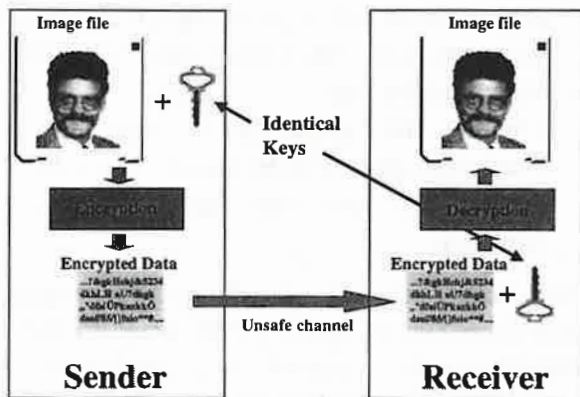


Figure 4: Principle of the symmetric encryption technique

Symmetric encryption procedures currently in widespread use include the following:

DES (Data Encryption Standard)

Block code with a key length of 64 bits (56 significant bits). This is the algorithm recommended by the US Bureau of Standards for commercial data encryption (was approved in 1981 as Data Encryption Algorithm, ANSI Standard X3.92-1981). Regarded due to its short key length as susceptible to cracking by high-powered computer systems. A document encrypted with DES 56 bit was cracked by the American Electronic Frontier Foundation in three days in 1998.

Triple DES

Plain text is DES-encrypted three times. The different available modes use either two or three different keys. Total key length depends upon the mode: 112 bits with two keys and 168 bits with three keys. Triple DES is regarded as one of the most effective methods of commercial data encryption. It is not only three times more secure than DES but, according to cryptographic experts, at least 2^{56} (10^{17}) times as secure as DES.

IDEA (International Data Encryption Algorithm)

Block code with a key length of 128 bits. Developed at the ETH Zurich. IDEA is patented in the US and in most European countries. The patent is held by the Swiss company Ascom Systec AG and is available for non-commercial use free of charge.

ASYMMETRIC ENCRYPTION TECHNIQUES

In asymmetric techniques (also known as public-key cryptosystems) each participant possesses two complementary keys –

- a public key (ordinarily the encryption key, accessible to all) and
- a private key (ordinarily the decoding key, to be kept secret).

Each key decodes the code generated with its complementary key. The secret (private) key cannot be derived from the public key. Thus the public key can be distributed via open networks and made public. Anyone can encrypt a message using a given recipient's public key, but only the recipient can decipher with his secret (private) key.

Asymmetric Encryption

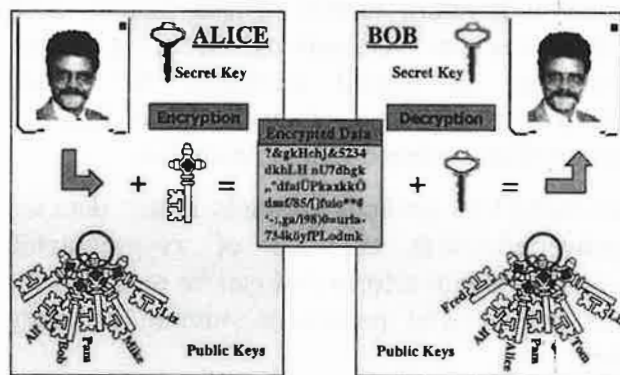


Figure 5: Principle of the asymmetric encryption technique

The most important asymmetric technique (RSA) is based upon the fact that it is relatively easy to multiply two prime numbers but extremely difficult to derive the original prime numbers from the product (computation of discreet logarithms). If the prime numbers selected are large enough, the problem of

negotiating the "mathematical one-way street" in the reverse direction becomes practically impossible to solve – at least within a reasonable period of time.

As a rule, all public keys are registered in publicly accessible files, whereas private keys are known only to their holders.

Advantages of asymmetric techniques:

- no need to exchange keys
- permit spontaneous contact with a partner
- 1001 participants = 2002 keys

Significant disadvantages of this type of encryption are the relatively heavy computation load and the correspondingly long computation times.

Asymmetric encryption techniques in current use include:

RSA (Rivest, Shamir, Adleman), 1978

In widespread use today is the system developed by Rivest, Shamir and Adleman in 1978 and named for its developers. The system uses a key length of 768 / 1024 bits. The RSA algorithms were published some time ago, and no mathematical weaknesses have been detected to date. The principle is based upon the difficulty of breaking down large natural numbers (e.g. 200 decimal places or 665 bits) into their prime factors. Numbers used in practical applications vary from 512 bits (low-grade security) and 2048 bits (very high-grade security). RSA is patented in the US (the patent expires in the year 2000) but not outside the US.

ElGamal, 1985

The principle of the ElGamal algorithm for asymmetric encryption is based upon the difficulty of computing "discreet logarithms on the model of a prime number". Numbers used in practical applications vary from 512 bits (low-grade security) and 1024 bits (very high-grade security). The algorithm is not patented.

Diffie-Hellmann, 1976

Diffie and Hellmann developed the first public-key encryption technique. The algorithm for the

exchange of public keys named after them is based (like ElGamal) on the problem of the "discreet logarithm". All patents have expired. The technique is to be implemented in France in connection with the introduction of a health-professional card.

Elliptical Curve Cryptosystems, 1985

This public-key process was developed by Miller and Koblitz. It involves the replacement of addition and multiplication of natural numbers with complex operations within a complicated mathematical structure (an elliptical curve). There are variations of Diffie-Hellmann and ElGamal for elliptical curves. These variations employ much shorter keys while providing an equivalent level of security.

HYBRID TECHNIQUES

Cryptographic systems used in public networks commonly combine the high encryption efficiency of symmetric techniques with the key-management advantages of asymmetric techniques in what are known as hybrid processes. In this method, the complete document is encrypted on the basis of the public key held by the recipient with a symmetric key (e.g. DES, 128 bits, created as a "session key" by the chip card processor using a random generator) and transmitted to the recipient. Only the session key is attached in encrypted form along with the recipient's public key (e.g. RSA, 1024 bits) to the document. The recipient first decodes the session key with his secret key; then, the entire document can be decoded with the symmetric key – much more rapidly than would be possible with the asymmetric key.

Ordinarily, software for such hybrid encryption functions can be installed in PCs intended for use in signature and verification operations in any number of networks for data transmission purposes.

II. The Digital Signature

The digital signature is a digital seal based upon a private signature key assigned by a

certification service provider⁸ (or TRUST centre: a trustworthy third-party authority) by means of a certification to a certain person.

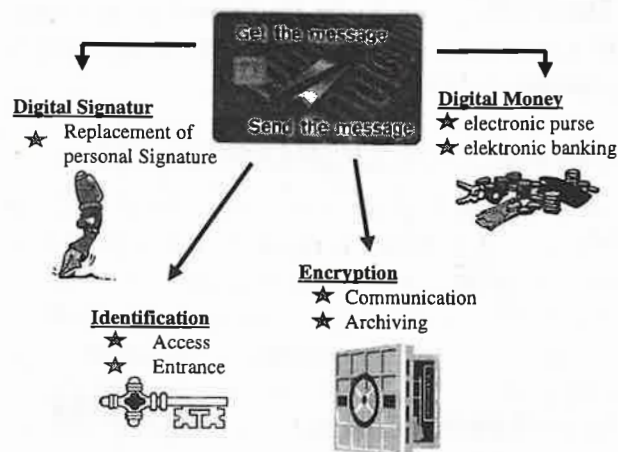


Figure 6: Application examples for digital signatures

THE HASH FUNCTION

A special mathematical function known as the hash function is needed to create a digital signature. Following a predefined process, it generates a check sum (hash total, also hash value, the document "fingerprint") from a plain-text passage of any length. The characteristics of the check sum are such that any change in the original text (no matter how slight) will produce a totally different hash value.

One of the requirements of this function is that the original text cannot be reconstructed on the basis of the hash value. In other words, the hash function is not reversible and is therefore regarded as a one-way or trapdoor function. This means – different from the case of encryption – that the original text cannot be reconstructed from the check sum.

Hash functions must be absolutely collision-free, meaning that the possibility of constructing two different messages that produce the same hash value must be ruled out. Thus with a negligible amount of uncertainty a certain hash value is the result of one and only one original plain text.

A hash function must be selected for the digital signature process. Currently available (one-way) hash functions include:

SHA/SHA-1 (Secure Hash Algorithm One)

SHA was developed by the NSA and accepted as a US Standard [SHA95]. A slightly modified form designated as SHA-1 has since replaced the original algorithm. The hash value generated by SHA-1 is required for the DSA (Digital Signature Algorithm) specified in the DSS (Digital Signature Standard). The hash value has a length of 160 bits.

MD2, MD4, MD5 (Message Digest)

MD4 and MD5 are hash functions [MD4, MD5] developed by R. Rivest (RSA Laboratories) and introduced in conjunction with the PEM standard (Privacy Enhanced Mail). MD5 is a further development of MD4. The algorithms generate a 128-bit message digest (hash value).

RIPEMD-128, RIPEMD-160 (RIPE Message Digest)

RIPEMD was developed by Hans Dobbertin, Antoon Bosselaers and Bart Preneel in the context of the EU RIPE project (RACE Integrity Primitives Evaluation, 1988-1992). The hash value can be 128 bits (RIPEMD-128) or 160 bits (RIPEMD-160) long.

Due to recognised weaknesses [RSA98], the RSA Data Security Inc. has ordered that MD4 and MD5, which are supposed to be collision-free, not be implemented. In general, hash functions with longer check sums offer a higher level of security. Therefore, SHA-1 or RIPEMD-160 should be used in the future. RIPEMD-160 appears to be establishing itself de facto as the European standard; SHA-1 is becoming the standard in the US.

THE INTEGRITY TEST

Generally speaking, hash functions are used to verify the integrity of texts (or data). The hash value is computed for a given text for this purpose. The hash value is then stored, either separately or together with the text (in which case it is given special security protection). If subsequent recomputation of the hash value for what is presumed to be the identical text

produces a different hash value, the text is presumed to have been falsified. Conversely, identical hash values confirm the identity of the data tested and thus the integrity of the text.

The advantage of this process lies in the fact that only a (relatively) short hash value must be stored or transmitted in a secure manner – and not the entire text. If such a hash process is openly disclosed and described to every user, any user can compute the hash value himself on the basis of the original plain text and determine, through comparison, whether the value transmitted by the sender is identical with his own result. In this way every user can check to determine whether a given hash result can actually be assigned to a specific message.

Integrity & Authenticity

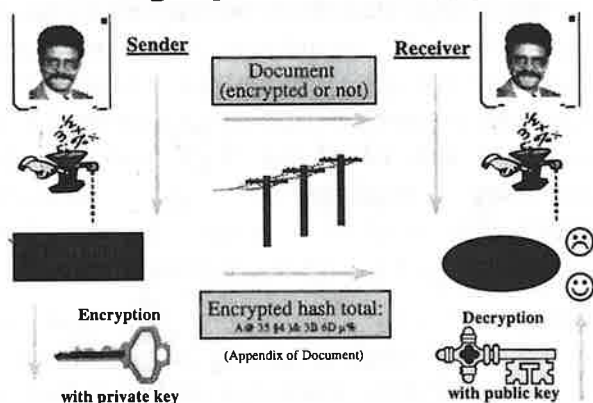


Figure 7: Principles of the integrity and authenticity test

THE AUTHENTICITY TEST

To verify the authenticity of a message, the sender encrypts the hash value of his message with his secret key, thus creating a digital signature. The recipient can verify this hash value following decoding (using the sender's public key) by hashing the message himself and determine whether the message was actually transmitted by the alleged sender. During the authentication process, the integrity of the message is automatically verified as well.

CERTIFICATION

Certifications confirm the authenticity of public keys. Among other things, a certification contains the name of the signature key holder, the public signature key assigned to the user, the dates of issue and expiration and the name

and signature of the issuing certification service provider⁸. It may also contain time-related, legal and/or financial restrictions. The certification is signed with the secret key of the issuing certification service provider.⁸ Thus it is also a digital ID for the user and can be tested for integrity and authenticity by anyone using the public key of the certification service provider. This supplementary function can be employed for the purpose of access authorisation or to reject undesired electronic mail.

A signed document consists of the document itself, the digital signature and, if needed, the (signature-key) certification of the signer. In cases where the recipient does not yet have possession of the sender's public key, the latter component is of crucial importance.

This certified digital signature offers several advantages:

- In essence, the signature is added to the document in the same manner as a handwritten signature.
- The signature process and the signature authenticity test can be completed quickly.
- The document cannot be reconstructed from the digital signature within a judicially relevant period of time.

If the recipient wishes to be sure that a given signature is currently valid, he can inquire online with the certification service provider at which the sender's key is registered.

This method ensures for the first time that data can be stored and/or transmitted electronically with a degree of security that is equal to or even exceeds that of conventional media – an aspect of data technology that is of great relevance to judicial proceedings.

III. The German Signature Act

The passage of the German Signature Act (SigG, as Article 3 of the Information and Communication Services Act, IuKDG) and the Signature Directive (SigV), the basic framework for the practical use of digital signatures was put into place. This legislation

establishes the requirements for forgery-proof signatures and manipulation-proof signed data.

The law includes provisions for a nation-wide infrastructure for the assignment of signature keys to natural persons, the use of suitable technical components (e.g. signature SmartCards, card readers, software) and user instruction with respect to safety precautions to be taken in their own interest.

The infrastructure is to be developed and operated by the private sector in a climate of open competition but under government regulatory control. This control function was assigned to the Regulatory Authority for Telecommunication and Mail (RegTP, headquarters in Mainz, in operation since 23 September 98) as the agency responsible for the practical implementation of the Signature Act.

The purpose of the law is to provide for a reliable basis – and thus for legal certainty – for the design of dynamically developing offerings in the field of information and communication services and to establish a balance between free market interests, the legitimate needs of users and the requirements of public order.¹²

The Federal Office of Security in Information Technology (BSI) was tasked with preparing catalogues of measures as a supplement to the SigG and the SigV. These catalogues of measures, developed in co-operation with business and scientific experts, contain specifications for technical components and security concepts for certification service providers. They are subject to continuous updating in response to the rapid pace of development in information technology. The goal is a high level of interoperability in the use of hardware and software produced by different manufacturers.

The SigG and the related implementation provisions specify that digital signatures must be based upon asymmetric encryption techniques. Among other things, the SigV contains detailed provisions governing the

certification process. Certification service providers are responsible for creating and certifying user keys and for maintaining public certification files. Certifications must bear an expiration date, and users must reapply for certification upon expiration. This requirement ensures that digital signatures whose security is already in jeopardy as a result of general technological developments are not regarded as forgery-proof indefinitely.

In addition, the SigV also specifies the minimum technical and organisational requirements that must be met by certification service providers and the basis upon which billing and accounting for their services are to be performed.

Digital signatures as defined in the SigG provide a high degree of security by virtue of the use of security-tested components (hardware and software) and the role played by certification service providers. Articles 14 of the SigG and 17 of the SigV prescribe the minimum requirements for technical components used to generate signature keys and to store and use private signature keys.

Required testing is to be performed by accredited IT security testing and certification service providers evaluated and certified in accordance with the ITSEC.¹³ Tests are designed to meet the security needs of the users in question, e.g. for private or commercial use. The ITSEC provide for certification of a low (E1), medium (E2 – E3) or high (E4 – E6) level of reliability with respect to the security functions of a given product. The signature chip card must meet the requirements for ITSEC certification level "E4 – high".¹⁴

These testing procedures are very time-consuming and thus expensive as well, a factor which influences the costs of the process as a whole.¹⁵ Besides the BSI, other organisations in the private sector can perform security testing

¹² Bundesamt für Sicherheit in der Informationstechnik, "Digitale Signaturen im Aufgabenspektrum des Bundesamtes für Sicherheit in der Informationstechnik".

¹³ Information Technology Security Evaluation Criteria.

¹⁴ In addition to the ITSEC security levels E1 – E6, the mechanism values "low", "medium" and "high" are indicated.

¹⁵ Evaluation costs for a chip card certified as "E4 – high" amount to about 250,000 DM.

for technical components in accordance with the ITSEC.

REGULATORY AUTHORITY AND CERTIFICATION SERVICE PROVIDERS

Trust is an essential prerequisite for interpersonal communication. Certification service providers are expected to establish a basis of trust with regard to the use of digital signatures. The term "certification service provider" was used deliberately in the language of the SigG because these institutions perform a somewhat different function than so-called trust centres. Certification service providers issue certifications, whereas trust centres ordinarily provide data encryption services.

Hierarchy of Authorities

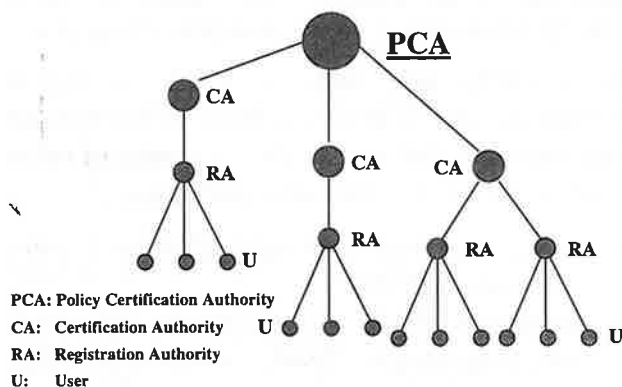
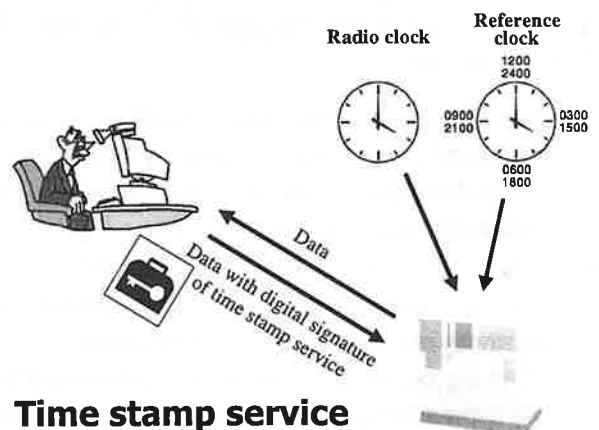


Figure 8: Hierarchy of the certification authorities

Certification service providers operate under the supervision of the RegTP (in accordance with Art. 66, TKG). The regulatory authority awards permits for certification service providers and supervises their operations. As the "root authority", certifies the public signature keys of the certification service providers. The certification service providers, in turn, certify the public signature keys of users upon completion of an identity check (presentation of a valid ID card).

Certification service providers can be by government agencies, associations and private sector organisations. Their responsibilities include:

- clearly identifying (e.g. on the basis of a German personal ID card) and registering signature applicants;
- generating a unique signature-key pair (if requested);
- issuing a certification, a digital certificate signed with the secret key of the certification service provider, on the basis of which a public key is assigned to a clearly identified person; the certification may contain time, legal and financial restrictions;
- personalising data, transferring certificates and, as appropriate, public and private keys to a signature component (ordinarily a SmartCard);
- maintaining an index of certifications with block notices, accessible online;
- issuing time stamps, an online service provided as confirmation that the certification service provider was in possession of certain data at a specific time;



Time stamp service

Figure 9: Time stamp service

- instructing users with respect to security in the use of digital signatures, e.g. proper handling of the data medium containing the private signature key, what to do in case of loss, PIN security, etc.

The recipient of a digitally signed document uses the sender's public key to verify the authenticity of the sender's signature. For this purpose, the recipient can check the signature of the certification service provider or verify the validity of the sender's public key by making an online inquiry in the index

maintained by the issuing certification service provider. Thus partners in communication who do not know one another place their trust in the care taken by the certification service provider in establishing the unmistakable identity of signature applicants. Although the SigG permits the issue of signature cards under pseudonyms, the certification service provider is required to register every applicant's real name.

The validity of the certification issued by the certification service provider can also be checked using the public key of the "root authority".¹⁶ Like the certification service providers, the root authority maintains an online index of all public keys registered for certification service providers.

In 1999, the Telekom subsidiary Telesec became the first certification service provider to issue signature cards along with the software and hardware required in accordance with the SigG and the SigV. The following components were made available through the Telekom "T-Punkt" outlets:

- the signature program "Secure Human Interface"; the program displays the signed or to-be-signed documents required for signature verification;
- a chip card reader (ITSEC "E4-high");
- a chip card as signature component; its contents include, among other things:
 - a signature key (secret key addressed by the signature program)
 - an encryption key, as appropriate, (secret key addressed by the encryption program).

A number of competitors have applied for approval as certification service providers. Prior to approval, the technical components and the security concept of the applicants must be tested/reviewed by accredited organisations authorised to issue such approval certificates. Currently authorised organisations include the BSI, debis Systemhaus Information Security Services GmbH, TÜV Informationstechnik

GmbH (Essen) and TÜV Product Service (Munich).¹⁷

IV. The European Guideline

The European Council passed a proposal for a "Common Framework for Electronic Signatures" on 22 April 99. The proposed guideline is now under deliberation in the European Parliament, and passage is expected in early 2000.

The EC Guideline differs in several ways from the German SigG. Basically, the draft proposal calls for a public-key system, and certification service providers are to be responsible for key management.

In contrast to the SigG, the EC proposal does not provide for a regulatory authority. The security requirements for the technical components employed are also less stringent.

It is likely that different kinds of digital signatures will be made available in Europe and that they will differ from the viewpoint of users with respect to both security and costs:

- electronic signatures (e.g. PGP as a pure software solution)
- advanced forms of electronic signatures (medium security level, viewed as the legal equivalent of a written signature)
- digital signatures as defined in the SigG (as a voluntary accreditation system offering a high degree of security)

In contrast to the SigG, the EC proposal contains liability provisions for certification service providers issuing advanced forms of electronic signatures.

V. The SmartCard: an information medium for sensitive data

Following magnetic-strip cards, SmartCards (chip cards containing microprocessors) represent the next generation of identification cards and offer a much broader range of applications. In addition to the features

¹⁶ <http://www.regtp.de/Fachinfo/Digitalsign/anerkstell2.htm>

¹⁷ Announcement regarding the digital signature as defined in the SigG and the SigV (9 February 98), *Bundesanzeiger* No.31, 14 February 98.

normally contained on a memory card, SmartCards are provided with a CPU and, if needed, a second processor used for encryption. These cards are freely programmable and provide password and encryption protection and thus a high degree of confidentiality for the data they contain.

Because of the relatively complex data protocol involved, the exchange of digital information via SmartCards ordinarily requires a connection to another computer, currently a PC in most cases. Some special, commercially available chip cards (cryptocards) capable of encrypting data and electronic documents may have a higher computing capacity than the PCs with which they communicate. The broad range of applications for chip cards also opens up a number of new possibilities of relevance to forensic science. For a discussion of other characteristics of chip cards we refer to the article "Die Chipkartentechnik aus kriminalistischer Sicht" [BKB97].

The signature card is also a special kind of chip card. In addition to the CPU, it also features a signature chip containing a private key (secure prior to being read out), the encrypted PIN and the entire manipulation-proof signature software. A fundamental security requirement is that the private key must not leave the chip card. It cannot be read out, and the signature chip cannot be duplicated.

For the purposes of the signature procedure, the PC computes the hash value¹⁸ of the document in question and loads it into the chip memory bank. There, the hash value is encrypted with the secret key and then linked to the document in the PC again. The hash function generates a compressed hash value with a fixed length (e.g. 160 bits) for every document (or block of data), regardless of its length. This value changes significantly with every alteration of the document, no matter how minor it may be.

The technical components required for the digital signature process are a PC (with signature software), a chip card reader and the signature chip card.

The Federal Ministry of the Interior currently plans to introduce a multi-purpose chip card with an identification function. As planned, this new official and facility ID card will permit the user to generate a digital signature, among other things. A pilot project is scheduled for launch in mid-2000. If the trial is successful, the identity card will be introduced step by step in subordinate departments as well and may even become mandatory for all government agencies.

VI. The Global Positioning System (GPS)

The GPS is a satellite-based navigation system developed under a 1973 US Department of Defence order by the Joint Program Office of the Los Angeles Air Force Base. The system was to have the capacity to determine the location and the speed of any stationary or moving object and to provide exact time information. Specifications required a system that would function under any and all weather conditions, at all times and at any given point on or near the earth's surface.

The result is a navigation system consisting of a total of 24 satellites which circle around the earth in six orbits at an altitude of approximately 20,200 km. Although conceived for military use, it now has a large and growing community of civilian users. System precision varies within a normal range of between 30 and 70 meters. The position data obtained through the GPS are routinely arbitrarily altered (rendered less precise) by the provider (the US) in order to make unauthorised military use more difficult.

The satellites transmit regular data signals on their exact position and, thanks to high-precision atomic clocks, synchronic time pulses. The GPS receiver on earth analyses the differences in travel time between the individual received signals. If a GPS receiver is located on a perpendicular directly below a satellite, signal travel time is approximately 70 milliseconds. If more time elapses, the receiver is obviously farther away, somewhere along an orbit running at a specific angle to a

¹⁸ See Appendix II. The Digital Signature.

perpendicular. The same applies to the signals received from a second satellite. Thus the GPS receiver must be located at one of the two orbit intersection points. The signal from a third satellite is needed for an exact determination of position.

Differential techniques are employed for the purpose of enhancing positioning precision in civilian applications. Distances between each satellite and a stationary GPS reference receiver are measured and computed at the same time. A comparison of the two different values produces the relevant DGPS correction data (Differential GPS) for each individual satellite. On the basis of this correction data, the GPS receiver operated by a user can reduce the uncertainty range of his positioning from ± 50 meters to less than ± 5 meters. The DGPS correction data are made available throughout Germany round the clock by Deutsche Telekom AG and the (German) Federal Office of Cartography and Geodesy (BKG).

Currently, satellite positioning systems use the GSM network (Global System for Mobile Communication) as a reasonably-priced data-transmission component. In the medium term, the low-altitude (approx. 800 and 1,400 km) Iridium and Globalstar satellite systems are to be made available. This will provide world-wide coverage and nearly 100-per-cent availability.

Use of the GPS will require that the camera be equipped with a chip set and an antenna. The advantages of the GPS are its continuous availability and its potential for global use. The disadvantages are the fact that the GPS does not always function reliably in buildings and that the receiver antenna will be difficult to integrate into the camera housing.

References

- [3DES85] ANSI X9.F.1, X9.52: Triple DES Modes of Operation, ANSI X9.17: Financial Institution Key Management Wholesale, American National Standards Institute, 1985
- [AG3-98] TeleTrusT Deutschland e.V.: Kryptographische Verfahren im

Gesundheits- und Sozialwesen in Deutschland – „Kryptoreport“, Erfurt, 1998

- [AG6-98] TeleTrusT Deutschland e.V.: Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren, Erfurt, 1998
- [Bae97] Manfred Bauer: Vermessung und Ortung mit Satelliten, Fourth Edition, Hüthig, Heidelberg, 1997
- [BKB97] Bundeskriminalamt, Kriminalistisches Institut: Die Chipkartentechnik aus kriminalistischer Sicht, Beilage zum Bundeskriminalblatt No. 247, Wiesbaden, 1997
- [CoCo98] Common Criteria for Information Technology Security Evaluation, Version 2.0, 1998
- [DiHe76] W. Diffie, M.E. Hellmann: New Directions in Cryptography, IEEE Transactions on Information Theory, 22, 1976
- [EFF98] Electronic Frontier Foundation, San Francisco, 1998, <http://www.eff.org>
- [FoWo97] D. Fox, P. Wohlmacher: Hardwaresicherheit von Smartcards, Datenschutz und Datensicherheit No. 5/1997, pp. 260, Wiesbaden, 1997
- [Hof94] Bernhard Hofmann-Wellenhof, Gerhard Kienast, Herbert Lichtenegger: GPS in der Praxis, Springer, Wien, New York, 1994
- [ITSEC91] Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), Vorläufige Form der harmonisierten Kriterien, Version 1.2, Bonn, 1991
- [IuKDG97] Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste – IuKDG Bundesgesetzblatt, Jahrgang 1997, Part I from 28.07.97, pp. 1870
- [MK97] Bundesamt für Sicherheit in der Informationstechnik: Entwurf Maßnahmenkatalog zur digitalen Signatur gem. SigV § 12 und § 16,

Draft of 19.11.1997 Version 1.0,
Bonn, 1997

[MD4] R. Rivest: The MD4 Message
Digest Algorithm, RFC1320, 1992

[MD5] R. Rivest: The MD5 Message
Digest Algorithm, RFC1321, 1992

[RIPE95] RIPE Consortium: Ripe Integrity
Primitives – Final Report of RACE
Integrity Primitives Evaluation
(R1040), Lecture Notes in
Computer Science, LNCS 1007,
Springer, 1995,
[http://www.esat.kuleuven.ac.be/~bo
sselaer/ripemd160.html](http://www.esat.kuleuven.ac.be/~bo
sselaer/ripemd160.html)

[RSA98] RSA Cryptography, FAQ
<http://www.rsa.com/rsalabs/newfaq/>

[SHA95] ANSI, „X9.30 Part 2: Secure Hash
Algorithm“, 1995; FIPS PUB 180-
1, NIST Federal Information
Processing Standards on Computer
Security (NIST FIPS),
<http://www.csrc.ncsl.nis.gov/fips>

[SigG] German digital signature law -
Gesetz zur digitalen Signatur
(Signaturgesetz – SigG) of
22.07.1997 (BGBI. IS. 1870, 1872),
promulgated as article 3 of IuKDG‘

[SigV] German signature regulations -
Verordnung zur digitalen Signatur
(Signaturverordnung – SigV),
Bundesgesetzblatt, Jahrgang 1997,
Part I, No. 70 of 27.10.1997, pp.
2498

[Spe98] Gabriele Spenger: Abschlußbericht
zur Projektstudie „Digitale
Bildaufzeichnung mit
Verschlüsselungseinheit“,
Fraunhofer Institut für Integrierte
Schaltungen, Erlangen, 1998

[Stro95] Jürgen Strobel: GPS Global
Positioning System, Franzis, Poing,
1995

[WJM94] William J. Mitchell: Digitale
Photomanipulation, Spektrum der
Wissenschaft, pp. 82 , 4/1994

Dr. Bernd Rieger
Bundeskriminalamt
Fachbereich KI 22
Thaerstr. 11
D-65173 Wiesbaden
Federal Republic of Germany
Tel.: +49-611-55-14204
Fax: +49-611-55-16274
e-mail: BR_KI_22@t-online.de

Harry Rode
Bundeskriminalamt
Fachbereich KI 24
Thaerstr. 11
D-65173 Wiesbaden
Federal Republic of Germany
Tel.: +49-611-55-14441
Fax: +49-611-55-16274
e-mail: HR_KI_24@t-online.de