Electronic Signatures

Authentication Technology from a Legal Perspective

Series Editors

For other titles in the Series see p. 150

INFORMATION TECHNOLOGY & LAW SERIES 5

ELECTRONIC SIGNATURES

Authentication Technology from a Legal Perspective

M.H.M. Schellekens

Center for Law, Public Administration and Informatization
Tilburg University

T•M•C•ASSER PRESS
The Hague

The *Information Technology & Law Series* is published
for IT*e*R by T·M·C·Asser press
P.O. Box 16163, 2500 BD The Hague, The Netherlands
<www.asserpress.nl>

T·M·C·Asser press English language books are distributed exclusively by:

Cambridge University Press, The Edinburgh Building, Shaftesbury Road,
Cambridge CB2 2RU, UK,
or
for customers in the USA, Canada and Mexico:
Cambridge University Press, 40 West 20th Street, New York, NY 10011-4211, USA

<www.cambridge.org>

The *Information Technology & Law Series* is an initiative of IT*e*R, the National Programme for Information Technology and Law, which is a research programme set up by the Dutch government and the Netherlands Organisation for Scientific Research (NWO) in The Hague. Since 1995 IT*e*R has published all of its research results in its own book series. In 2002 IT*e*R launched the present internationally orientated and English language *Information Technology & Law Series*. This series deals with the implications of information technology for legal systems and institutions. It is not restricted to publishing IT*e*R's research results. Hence, authors are invited and encouraged to submit their manuscripts for inclusion. Manuscripts and related correspondence can be sent to the Series' Editorial Office, which will also gladly provide more information concerning editorial standards and procedures.

Editorial Office
NWO / IT*e*R
P.O. Box 93461
2509 AL The Hague, The Netherlands
Tel. +31(0)70-3440950; Fax +31(0)70-3832841
E-mail: <iter@nwo.nl>
Web site: <www.nwo.nl/iter>

Single copies or Standing Order
The books in the *Information Technology & Law Series* can either be purchased as single copies at the regular retail price or through a standing order at a discount. For ordering information see the information on top of this page or visit the publisher's web site at <www.asserpress.nl/cata/itlaw5/fra.htm>.

ISBN-13 978-90-6704-174-4 hardback
ISBN-10 90-6704-174-2 hardback
ISSN 1570-2782

Cover and lay-out: Oasis Productions, Nieuwerkerk a/d IJssel, The Netherlands
Printing and binding: Koninklijke Wöhrmann BV, Zutphen, The Netherlands

TABLE OF CONTENTS

Abbreviations		VII
One	**Introduction**	1
1.1	Introduction	3
1.2	Defining the Problem	4
1.3	Outline	6
Two	**Authentication Technology: an Elementary Explanation**	9
2.1	Introduction	11
2.2	Authentication Within the Internet	11
2.3	Dedicated Means of Authentication	15
2.4	Public Key Encryption	25
2.4.1	Public key encryption in general	25
2.4.2	Certification	28
2.4.3	PKI-based authentication mechanisms	41
2.4.4	Technologies covering partial aspects	49
Three	**Usability of Authentication Technology**	53
3.1	Introduction	55
3.2	Qualification as a Signature	55
3.2.1	Forms of recognition	55
3.2.2	The functions of a signature	59
3.2.3	Performing the functions with the help of technology	71
3.2.3.1	Technologies for network identification	72
3.2.3.2	Passwords and PINs	73
3.2.3.3	Biometric technology	74
3.2.3.4	Symmetric encryption	76
3.2.3.5	Digital signatures	77
3.2.3.6	SSL and TLS	79
3.2.3.7	Timestamps and Cards	80

3.2.4	The functions of and qualification as a signature	80
3.2.5	What is beyond functional equivalence?	81
3.3	Evidentiary Value	89
3.4	Semi-legal Considerations of Usability	94
Four	**Misuse and the Burden of Proof**	99
4.1	Introduction	101
4.2	The Division of Risks	101
4.3	The Division of the Burden of Proof	111
Five	**Privacy Implications of the Use of Electronic Signatures**	117
5.1	Why Privacy?	119
5.2	Digital Signatures	121
5.2.1	Personal data?	121
5.2.2	The processing of personal data	123
5.3	Symmetric Encryption	125
5.4	Biometrics: the Dynamic Signature or Signature-scan	126
5.5	Conclusion	128
Six	**Conclusion**	131
Literature		143
Appendix		147
Index		148

ABBREVIATIONS

ABA	American Bankers Association
ACL	Access Control List
ADR	Alternative Dispute Resolution
AES	Advanced Encryption Standard
ANSI	American Natonal Standard Institute
ATM	Automatic teller machine
BBL	Bolero Bill of Lading
CA	Certification Authority
CMI	Comité Maritime Internationale
CPS	Certification Practise Statement
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSP	Certification Service Provider
DCC	Dutch Civil Code
DCCP	Dutch Code of Civil Procedure
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DOI	Digital object identifier
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DTD	Document Type Declaration
EDI	Electronic Data Interchange
ETSI	European Telecommunications Standard Institute
FIPS	Federal Information Processing Standard
HR	Hoge Raad

ICT	Information and Communication Technology
ID	Identification number
IETF	The Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ISDN	Integrated Services Digital Network
JILT	Journal of Information Law & Technology
KPN	The main (incumbant) Dutch telecom operator
Ktg.	Dutch Summary Court (Kantongerecht)
LAN	Local Area Network
MAC	Message Autentication Code ch. 2
MAC address	Media Access Layer address
MIME	Multipurpose Internet Mail Extensions
MOSS	MIME Object Security Services
NJ	Dutch case law reference
NJB	Nederlands Juristenblad
NRD	Non-Refutable Document
ODR	On-line Dispute Resolution
PEM	Privacy Enhanced Mail
PIN	Personal Identification Number
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
RA	Registering Authority
RIPE	Réseau IP Européen
RSA	Encryption method (by Rivest, Shamir and Adleman)
RvdW	Rechtspraak van de week
SCOS	Smartcard operating system
SET	Secure Electronic Transactions

SDSI	Simple Distributed Security Infrastructure
SIDN	Stichting Internet Domein Namen
SKIP	Simple Key Management for Internet Protocols
SPKI	Simple Public Key Infrastructure
SSL	Secure Socket Layer
S2ML	Security Service Markup Language
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSA	Time Stamping Authority
TTP	Trusted third party
UNCITRAL	UN Commission on International Trade Law
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
USB	Universal Serial Bus
WORM	Write Once Read Many
WPNR	Weekblad voor Privaatrecht, Notariaat en Registratie
WTLS	Wireless Transport Layer Security
WWW	World Wide Web
XML	eXtensible Markup Language