

Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

1854

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

G rard Lacoste Birgit Pfitzmann
Michael Steiner Michael Waidner (Eds.)

SEMPER - Secure Electronic Marketplace for Europe



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Gérard Lacoste
Compagnie IBM France, Centre d'Etudes et Recherches
Le Plan du Bois, 06610 La Gaude, France
E-mail: lacoste@fr.ibm.com

Birgit Pfitzmann
Universität des Saarlandes, Fachbereich Informatik
Im Stadtwald, 66123 Saarbrücken, Germany
E-mail: pfitzmann@cs.uni-sb.de

Michael Steiner
Michael Waidner
IBM Zurich Research Laboratory
Säumerstrasse 4, 8803 Rüschlikon, Switzerland
E-mail: steiner@acm.org, wmi@zurich.ibm.com

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

SEMPER - secure electronic marketplace for Europe / Gérard Lacoste ...
(ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ;
London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2000
(Lecture notes in computer science ; Vol. 1854)
ISBN 3-540-67825-5

CR Subject Classification (1998): E.3, C.2, D.4.6, K.4.4, K.6.5, J.1

ISSN 0302-9743

ISBN 3-540-67825-5 Springer-Verlag Berlin Heidelberg New York

SEMPER is part of the European Commission's ACTS Programme (Advanced Communications Technologies and Services). Funding is provided by the partner organisations, the European Union, and the Swiss Federal Department for Education and Science.

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag is a company in the BertelsmannSpringer publishing group.
© Springer-Verlag Berlin Heidelberg 2000
Printed in Germany

Disclaimer: Some of the systems mentioned in this book may be protected by trademarks, copyrights, or patents. They are the property of their owners.

Typesetting: Camera-ready by author
Printed on acid-free paper SPIN: 10722159 06/3142 5 4 3 2 1 0

Foreword

Some years ago, businesses could choose whether to migrate to electronic commerce, however, today it seems they have no choice. Predictions indicate that companies that do not make the necessary changes will be overrun by competition and ultimately fail. Therefore, we see more and more companies undergoing tremendous transformation in order to adapt to the new business paradigm. At the same time new companies are being established. One thing these companies have in common is the increased dependency on security technology. The invention of electronic commerce has changed the role of security technologies from being merely a protector to being also an enabler of electronic commerce, and it is clear that the development of security technology is a key enabler in the growth and deployment of electronic commerce. This has been recognised at European level (European Union 1997e).

The launch of a comprehensive EU policy in the area of security in open networks is fairly recent with the adoption of a Communication on cryptography in October 1997 (European Union 1997c). A very important complement and support to the European policy is the European Commission's contribution to overcome technological barriers by giving special importance to R&D (Research and Development) activities.

The *SEMPER* project was launched in September 1995 and was funded partly by the European Community within the *Advanced Communication Technologies and Services* (ACTS) specific research programme part of the Fourth Framework Program (1994-1998). In this book the *SEMPER* project team presents in a coherent, integrated, and readable form the issues addressed, the motivation for the work carried out, and the key results obtained.

SEMPER is an innovative project in several aspects. What really makes it innovative and impressive is the integration of the following components into an overall security framework for electronic commerce:

- *SEMPER* is the first project aiming at securing electronic commerce as a whole by developing a technical security framework realised as a middleware. This brings forward two advantages. First, such a technical security framework supports multiple business scenarios by providing powerful security services to applications implementing the business processes. A novelty compared to other security middleware is the provision of security mechanisms through a more commerce-oriented application programming

- interface. Second, the development environment shields application designers from the security implementation details and their evolution over time.
- *SEMPER* provides an open security platform which can be configured with relevant modules in order to cope with national regulations.
 - A trustworthy user interface, TINGUIN, which ensures that users can securely manage information. TINGUIN provides a single point of interaction between users and their secure platform. Such a single interface is essential to ensure users' consistent perception of their security.
 - *SEMPER* has proposed a legal framework for establishing legal predictability of electronic commerce. An interesting result is the adaptation of the technical and legal frameworks to each other by enabling the user's tools to visualize important legal aspects and to manage legal parameters.

The results in this book constitute a major contribution to the development of secure electronic commerce and the work presented has set the scene for future directions in secure electronic commerce. The last chapter of the book highlights some open problems related to the work done by the project. However, many more exist and there is still a lot to be done before the goal of secure electronic commerce will be reached. This has been recognised at European level, and the security-related R&D activities will be intensified under the new 5th Framework Program (1998–2002). Within the 5th Framework Program, the Information Society Technology (IST) Programme addresses the technologies of the online world.

Everyone interested in investigating the state of the art and future directions for secure electronic commerce should find this book extremely valuable and it is without any reservation that I strongly recommend it.

May 2000

Spyros Konidaris
European Commission
Director a.i. – DG XIII-F

Preface

Since the invention of the World-Wide Web (WWW) in 1991, Internet-based electronic commerce has been transformed from a mere idea into reality. Customers browse through catalogues, search for best offers, order goods, and pay for them electronically. Information services can be subscribed online, and many newspapers and scientific journals are readable via the Internet. Most financial institutions have some sort of online presence, allowing their customers to access and manage their accounts, make financial transactions, trade stocks, and so on. Some countries already support filing tax declarations electronically. Electronic mails are exchanged within and between enterprises and often already replace fax copies. Soon there will be no enterprise left without some Internet presence, if only for advertisement reasons. In early 1998 more than 2 million web servers were connected to the Internet, and more than 30 million host computers (Zakon 1998). Internet business is estimated to have reached \$50 to \$100 billion in 1998, mostly in business-to-business trade, and continues to increase at a high rate of growth (Henry, Cooke, Buckley, Dumagan, Gill, Pastore, and LaPorte 1999).

Thus, doing some electronic business on the Internet is already an easy task. As is cheating and snooping. Several reasons contribute to this insecurity. The Internet does not offer much security per se. Eavesdropping and acting under false identity is simple. Stealing data is undetectable in most cases. Popular PC operating systems offer little or no security against viruses and other malicious software, which means that users cannot even trust the information displayed on their own screens. At the same time, user awareness of security risks is threateningly low.

The only well-accepted security tool for the World-Wide Web is the Secure Sockets Layer protocol (SSL), which provides a secure pipe between web client and web server (Freier, Karlton, and Kocher 1996). It cannot generate signed messages or signed receipts, which naturally makes it unsuitable to tasks like electronic online payments and contract signing. And even for SSL, the problem of *visualizing* security to the user is unsolved: most WWW browsers only distinguish between “secure” and “insecure” connections, but do not tell the users in a simple way with *whom* exactly they are communicating over an established “secure” channel.

Such user interface problems are amplified by the fact that today's electronic-commerce systems offer little support in maintaining consistency in data and security among the different parts of a business process. As in the paper world, users have to fill in the same data again and again, copy data on several forms, accumulate data from different transactions by hand, and so on. More problems are revealed if one looks at the legal aspects: often it is not clear—or not even decided—who bears liability and which country's law is applicable in a specific situation.

In 1994 we, the *SEMPER* consortium, came up with the idea that all these security problems could best be solved by grouping all necessary security technologies under a coherent and open software framework, and a single, consistent user interface. Such a framework should allow automatic linking of parts of a business process. Necessarily, it should support not only secure communication and payments, but also the negotiation of business and security parameters, fair exchange of documents (as in contract signing and certified mail), handling of disputes among the parties, etc. Besides keeping data confidential, it should also grant its users some degree of anonymity and unobservability—like users on physical marketplaces can act anonymously. All this should be based on requirements from the market, and should be consistent with the legal systems.

The idea was turned into a proposal to the European Commission, with the result that we started work on implementing this idea in September 1995. We concluded the project early 1999. Some partners are currently exploiting parts of *SEMPER*, but we also aim at more complete use of the framework in successor projects and products. This book summarizes our main results.

Part I gives an overview of our solutions, i.e., the technical framework and a proposal how to tackle the open legal questions. This part is intended to be readable by everyone, i.e., it does not presuppose a specific technical background except some basic familiarity with the Internet.

Part II covers topics for which fundamentally new scientific or engineering results were obtained, and looking at them in detail would be beneficial to everybody working in the field. See the introduction of Part II for more details.

The results of *SEMPER*, including the full architecture, prototype description, and results from expert surveys and trial evaluations, are documented in a number of public, formal deliverables. These are available online from <http://www.sempor.org>, or by writing to: IBM Zurich Research Laboratory, Computer Science Department/Project *SEMPER*, Säumerstrasse 4, CH-8803 Rüschlikon, Switzerland.

May 2000

*Gérard Lacoste
Birgit Pfitzmann
Michael Steiner
Michael Waidner*

Authors of this report: Part I was written, based on the results of the entire project, by *Birgit Baum-Waidner, Gérard Lacoste, Birgit Pfitzmann, Michael Steiner, Michael Waidner, and Arnd Weber*. Chapter 5 was written by *Michael Waidner*. Chapter 6 was written by *N. Asokan, Birgit Baum-Waidner, Torben P. Pedersen, Birgit Pfitzmann, Matthias Schunter, Michael Steiner, and Michael Waidner*. Chapter 7 was written by *Dale Whinnett and Reinder Wolthuis*. Chapter 8 was written by *Akis Hamamtzoglou, Thomas Hecht, Giannis Papadopoulos, and Arnd Weber*. Chapter 9 was written by *Rolf Michelsen, Stig Mjølunes, Petros Pantis, and Kostas Tzelepis*. Chapter 10 was written by *Matthias Schunter*. Chapter 11 was written by *N. Asokan and Michael Steiner* and is based on (Abad-Peiro, Asokan, Steiner, and Waidner 1998; Asokan 1998; Asokan, Herreweghen, and Steiner 1998). Chapter 12 was written by *Maria Gatziani, Torben P. Pedersen, and Kambiz Zangeneh*. Chapter 13 was written by *Birgit Baum-Waidner*. Chapter 14 was written by *Birgit Baum-Waidner and Rita Zihlmann*. Chapter 15 was written by *Michael Waidner*.

People and organizations who contributed to *SEMPER*: *Fabrice Clerc, Philippe Magliulo, Marc Mazoué, and Marie-Jo Revillet* from CNET - France Télécom. *Holger Erichsen and Bernd Horsch* from the Commerzbank. *Bjarke Dahl Ebert, Maria Gatziani, Peter Landrock, Kim Lueders-Jensen, Timmy G. Madsen, Jesper Drud Nielsen, Thomas Sepstrup Nielsen, and Torben P. Pedersen* from Cryptomathic. *Paul Dinnissen, Berry Schoenmakers, and Bryce Wilcox* from Digicash. *Akis Hamamtzoglou, John Katakis, Sophia Koutsoukou, Dimitrios Livas, and Giannis Papadopoulos* from EURO-COM EXPERTISE. *Christoph Baert, John Schey, and John West* from Europay International. *Michael Ehrl, Thomas Hecht, and Ralf Kuron* from FOGRA Forschungsgesellschaft Druck e.V.. *Horst Ehmke, Matthias Enzmann, Rüdiger Grimm, Tobias Himstedt, Basawarai Patil, Wolfgang Putz, and Kambiz Zangeneh* from the Forschungszentrum Informationstechnik mbH (GMD). *Jean-Marie Blanchère, Sylvain Cornillon, Gerard Lacoste, Philippe Leblanc, Jean-Pierre Le Heiget, and Christian Navarro* from IBM France, Centre d'Études et Recherches; *Ulrich Einig, Karsten Riede, and Christian Thiel* from IBM Heidelberg; *Jose L. Abad-Peiro, N. Asokan, Andreas Fleuti, Ceki Gülcü, Günter Karjoth, Ferdinando Loiacono, Mehdi Nassehi, Thomas Schweinberger, Michael Steiner, Els van Herreweghen, and Michael Waidner* from IBM Research, Zürich. *Petros Pantis, Maria Tsakali, and Kostas Tzelepis* from INTRACOM. *Sylvain Cornillon, Sharon Prins, Jako Swanenburg, Matthijs de Vries, and Reinder Wolthuis* from KPN Research Netherlands. *D.M.A. Schaap* from MARIS. *Mathias Flenker, Stefan Liesem, Christian Petersen, and Ingo Saleck* from Otto Versand. *Mogens Rom Anderson, Birgit Baum-Waidner, Klaus Becker, Felix Jaggi, Thomas Mittelholzer, Armin Müller, Claus Rasmussen, Rainer Rueppel, Bruno Wildhaber, and*

Rita Zihlmann from Entrust/r3 security engineering ag. *Rolf Michelsen* and *Stig Frode Mjølunes* from SINTEF Telecom and Informatics. *Peter Bosch*, *Dick Bulterman*, *Ray Hirschfeld*, *Jaap Henk Hoepman*, *Sjoerd Mullender*, and *Louis Salvail* from the Stichting Mathematisch Centrum (CWI). *Matthias Schunter* from the Universität Dortmund. *Ingo Pippow*, *Jan Reichert*, *Arnd Weber*, and *Dale Whinnett* from the Universität Freiburg, Institut für Informatik und Gesellschaft. *Birgit Pfitzmann* and *Matthias Schunter* from the Universität Hildesheim, Institut für Informatik. *Tom Beiler*, *Jürgen Brauckmann*, *Lothar Fritsch*, *Birgit Pfitzmann*, and *Matthias Schunter* from the Universität des Saarlandes, Saarbrücken, Fachbereich Informatik. Sponsoring partners of *SEMPER* were Banksys (Belgium), Banque Générale du Luxembourg (Luxembourg), Enyca (Spain), and Telekurs/Payserv (Switzerland). The project was led by IBM.

The following organisations provided the infrastructure for the *SEMPER* trials: in France: ACRI, Actimedia, Centre d'Études et Recherches IBM France, Centre International de Communications Avancées, France-Télécom, and IDATE; in Germany: Commerzbank, FOGRA Forschungsgesellschaft Druck e.V., Forschungszentrum Informationstechnik mbH (GMD), Gesellschaft für Zahlungssysteme (GZS), Otto Versand, Universität Freiburg, Institut für Informatik und Gesellschaft, and Universität des Saarlandes, Saarbrücken, Fachbereich Informatik; in Greece: EUROCOM EXPERTISE; in The Netherlands: KPN Research, MARIS, and Stichting Mathematisch Centrum (CWI); in Switzerland: IBM Research, Zürich; in the UK: Oil and Gas Product Library Ltd. (OPL); in the USA: GTE; and the members of the MOMENTS consortium.

SEMPER was part of the Advanced Communication Technologies and Services (ACTS) research program established by the European Commission for 1994-1998, and received funding under contract *AC026* from the European Commission DGXIII and the Swiss Bundesamt für Bildung und Wissenschaft.

Acknowledgments: Interesting discussions with several people outside the consortium helped us to develop and to refine the ideas presented in this book. In particular, we would like to thank *Alain André*, *Patrick Aubry*, *Ali Bahreman*, *Philippe Bardet*, *Annarosa Baum*, *Joachim Biskup*, *Jay Black*, *Michel Bosco*, *Peter Büttner*, *Mario Campolargo*, *David Chaum*, *Anne Clarke*, *Marc Dacier*, *Michel Dauphin*, *Michel Fossaert*, *Renaud di Francesco*, *Michel Frenkiel*, *Philippe Garnesson*, *Mark Greene*, *Phil Janson*, *Spiros Konidaris*, *Jens Kristensen*, *Philippe Lefevbre*, *Karine Lieres*, *Mark Linehan*, *Jean-Pierre Meyer*, *Refik Molva*, *François Montagner*, *Kostas Papanikolaou*, *Peter de Rooij*, *Paul Rottier*, *Jukka Salo*, *Boris Saulnier*, *Tom Scanlan*, *Julia Sime*, *Hansrudolf Thomann*, *Paul Timmers*, *Gene Tsudik*, *Joep Van de Veer*, *Pierre Vannel*, *Hans-Dieter Zimmermann*, and *Rosalie Zobel*.

Table of Contents

Part I. The Vision of *SEMPER*

1. Secure Electronic Commerce	3
1.1 The Notion of “Electronic Commerce”	3
1.1.1 Example 1: Shopping over the Internet	3
1.1.2 Example 2: Business-to-Business Commerce	5
1.2 What’s Special about Electronic Commerce?	6
1.2.1 Virtuality of Electronic Commerce	6
1.2.2 The Internet as a Hostile Environment	6
1.2.3 Insecure User Equipment	7
1.2.4 New Opportunities to Commit Fraud	8
1.3 Existing Approaches to Secure Electronic Commerce	8
1.3.1 Secure Channels	8
1.3.2 Trusted Market Provider	9
1.3.3 Digital Signatures and Public-Key Infrastructures...	10
1.3.4 Payment Systems	11
1.4 The Whole Picture of Electronic Commerce	11
1.5 Resulting Goals of <i>SEMPER</i>	13
1.5.1 Security Requirements	13
1.5.2 The <i>SEMPER</i> Focus	13
2. Technical Framework	15
2.1 The <i>SEMPER</i> Model	15
2.2 Approach	17
2.3 Architecture	18
2.4 Protocols and Implementation	21
3. Legal Framework	23
3.1 Introduction	23
3.2 Predictable Liability for Signature Keys	24
3.2.1 Commitments without Online Third Party	25
3.2.2 Liability-Cover Service	25
3.2.3 Security and Market Effectiveness	26
3.3 The <i>SEMPER</i> Electronic-Commerce Agreement	27
3.3.1 Structure of <i>SECA</i>	27

3.3.2	Introducing Electronic-Commerce Agreements	28
3.4	Conclusions	29
4.	Vision of Future Products	31
4.1	Four Facets of <i>SEMPER</i> as a Product	31
4.2	<i>SEMPER</i> -based Business Applications	33
4.2.1	Secure Internet Shopping	33
4.2.2	Person-to-Person Scenario: The Fair Internet Trader	34
4.3	Outlook	37

Part II. Project Achievements

5.	Organizational Overview	41
5.1	Structure of <i>SEMPER</i>	41
5.2	Lessons Learned	42
5.2.1	Initial Education	42
5.2.2	Common Understanding	42
5.2.3	Teams of Individuals, not Organizations	42
6.	Architecture	45
6.1	Important Concepts	45
6.1.1	The Model of Deals, Transfers, and Exchanges	45
6.1.2	Global Security Concepts	46
6.1.3	Security Attributes	48
6.1.4	Transactions, Sessions, Contexts	48
6.2	Service Architecture	49
6.2.1	Business Applications	49
6.2.2	Commerce Layer	51
6.2.3	Transfer-and-Exchange Layer	52
6.2.4	Business-Item Layer	54
6.2.5	Supporting Services	55
6.3	Implementation Architecture	58
6.3.1	Structure of a Block: Manager-Module Concept	58
6.3.2	Communication	60
6.3.3	Business Applications and Browser Integration	61
6.4	Prototype	61
6.5	Outlook	62
7.	Experiments	65
7.1	Introduction	65
7.2	Trial Sites and Services	66
7.2.1	Internal <i>SEMPER</i> Trials	68
7.2.2	Freiburg Basic Trial	69
7.2.3	SME Trials	70

7.2.4	Freiburg SME Trial	74
7.2.5	MOMENTS Trial	74
7.3	Trial Implementations	74
7.3.1	Trial Services	75
7.3.2	Equipment and Set-Up	76
7.3.3	SME Business Applications	77
7.3.4	MOMENTS Trial	77
7.4	Trial Participants' Reactions	77
7.4.1	Initializing the <i>SEMPER</i> Software	78
7.4.2	Purse Creation and Management/Payment Options	80
7.4.3	TINGUIN (Trustworthy User Interface)	82
7.4.4	Secure Identification and Document Exchange	84
7.5	Service Providers' Reaction	85
7.6	Conclusion	91
8.	The Fair Internet Trader	95
8.1	Vision of a Person-to-Person Electronic-Commerce Tool	95
8.1.1	A New Type of Electronic Commerce	95
8.1.2	The Role of a Tool	96
8.2	The FIT from a User Perspective	97
8.2.1	Overview	98
8.2.2	Negotiation Stage	98
8.2.3	Contract Signing Stage	102
8.2.4	Fulfillment Stage	103
8.2.5	Disputes	105
8.3	Internal Design	106
8.3.1	Overview	106
8.3.2	The Messages Subsystem	108
8.3.3	The Display Subsystem	108
8.3.4	The Flow Subsystem	109
8.3.5	Execution Model	111
8.4	Experiments	113
8.5	Outlook	119
9.	The Commerce Layer: A Framework for Commercial Transactions	121
9.1	Technical Approach	121
9.1.1	The Challenge	121
9.1.2	The Generic Deal Approach	122
9.2	Concepts and Architecture	124
9.2.1	The Commerce-Transaction Service Model	124
9.2.2	Trust Relations	126
9.2.3	Commerce Transaction	127
9.2.4	Commerce Deal	127
9.2.5	The Commerce Service API Access Control	129

9.2.6	Authorization of Commerce Transactions	130
9.2.7	Service Quality Management	135
9.3	Design Overview	136
9.3.1	The Commerce-Layer Use Cases	136
9.3.2	Class Diagram.....	139
9.3.3	Commerce Transactions	141
9.3.4	Representation of a Commerce Transaction	141
9.3.5	The Downloader	141
9.3.6	Scenarios	146
9.4	Using the Commerce Transaction Service	148
9.4.1	Case Description.....	149
9.4.2	Definition of Transaction Classes	149
9.4.3	Activation of a Deal.....	151
9.4.4	Inspection of a Deal.....	152
9.4.5	Commerce Transactions	152
10.	Fair Exchange: A New Paradigm for Electronic Commerce	155
10.1	Introduction and Overview	155
10.1.1	Why “Generic” Fair Exchange?.....	156
10.1.2	Overview	158
10.1.3	Notation and Assumptions	158
10.2	Related Work	159
10.2.1	Certified Mail	159
10.2.2	Contract Signing	160
10.2.3	Fair Purchase	161
10.3	Using Transfers and Fair Exchanges	162
10.3.1	Transfers of Basic Business Items	163
10.3.2	Fair Exchange	163
10.4	A Model of Transfers Enabling Fair Exchange	164
10.4.1	External Verifiability	164
10.4.2	Generatability	166
10.4.3	Revocability	168
10.4.4	Examples	169
10.5	Transfer-based Generic Fair Exchange.....	170
10.5.1	Exchanging Externally Verifiable and Generatable Items	170
10.5.2	Exchanging Externally Verifiable and Revocable Items	172
10.5.3	Efficiency	172
10.6	The <i>SEMPER</i> Fair-Exchange Framework	173
10.6.1	Class Hierarchy.....	174
10.6.2	The Transfer-and-Exchange Framework in Action ...	178
10.6.3	Extending the Transfer-and-Exchange Layer.....	182

11. The Payment Framework	185
11.1 Introduction	185
11.2 Models of Electronic Payment Systems	187
11.2.1 Players	187
11.2.2 Payment Models	188
11.3 Design of the Framework	189
11.3.1 Scope	189
11.3.2 Functional Architecture	189
11.3.3 Design Overview	193
11.3.4 Purses	195
11.3.5 Transactions and Transaction Records	195
11.3.6 Payment Manager	197
11.4 Adapting a Payment System	198
11.5 Using the Generic Payment Service Framework	199
11.5.1 Payment Transactions	199
11.5.2 Special Application Functionality	201
11.6 Token-based Interface Definition	201
11.7 Extending the Design	204
11.7.1 Dispute Management	204
11.7.2 Payment Security Policies	207
11.8 Related Work	210
11.9 Summary	211
12. Trust Management in the Certificate Block	213
12.1 Public-Key Infrastructure	213
12.2 The Need for Trust Management	216
12.2.1 Specifying Trusted CAs and Acceptable Certificates	218
12.2.2 Selecting Certificates Automatically in a Business Session	218
12.3 Design of Policy Management	220
12.3.1 Maintaining Information about Policies	220
12.3.2 Using Policies	220
12.3.3 Negotiation of Certificates	222
12.4 Prototype Implementation	223
12.4.1 Public-Key Infrastructure in the <i>SEMPER</i> Trials	223
12.4.2 Trust Management	225
12.5 Related Work	230
12.5.1 Netscape Communicator	230
12.5.2 Microsoft Internet Explorer	231
12.5.3 PolicyMaker	232

13. Limiting Liability in Electronic Commerce	233
13.1 Introduction	233
13.1.1 Necessity to Limit Liability	233
13.1.2 Separation Between Digital Signature and Undeniable Commitment	237
13.1.3 Principles and Achievements of the Solution Proposed	239
13.2 Description of the Commitment Service	240
13.2.1 What Exactly is an Undeniable Commitment?	241
13.2.2 Initialization of the Subscriber	242
13.2.3 Key Certificate	243
13.2.4 Key Revocation	244
13.2.5 Commitment Request and Response	244
13.2.6 Validity of the Commitment Certificates	246
13.2.7 Using the Commitment Service as Liability-Cover Service	246
13.2.8 Integration in a Legal Framework	247
13.3 Possible Variants and Supplements	247
13.3.1 Limits	248
13.3.2 Message Flow	248
13.3.3 Combination with “Solvency Service”	249
13.3.4 Recharging Liabilities	249
13.3.5 Several Relying Parties or Beneficiaries	250
13.3.6 Other Kinds of Authorization and Issuance of Commitment Certificates	251
13.4 Who is Liable for Failures at the CCA?	252
13.5 Conclusions	253
13.5.1 Reasons for Merchants to Use the Commitment Service	253
13.5.2 Chambers of Commerce to Provide the Commitment Service?	254
13.5.3 Reasons for Buyers to Use the Commitment Service	254
14. Legal Aspects	257
14.1 Introduction	257
14.2 Legal Issues in Electronic Commerce	258
14.2.1 Applicable Law and Jurisdiction	259
14.2.2 Electronic Authentication—Validity of Digital Signatures	260
14.2.3 Proof of Digital Signatures	260
14.2.4 Regulations for Use and Export of Dual-Use Goods	262
14.2.5 Consumer-Protection Laws	263
14.2.6 Privacy and Data Protection	263
14.2.7 Advertising, Competition, Spamming	264
14.2.8 Content of Contracts and Internet Pages	265
14.2.9 Contract Law	266
14.2.10 Copyright and Trademark	267

14.2.11	Payment	269
14.2.12	Taxation	270
14.2.13	Conclusions	270
14.3	Selected Approaches at Legal Frameworks	270
14.3.1	UNCITRAL Model Law on Electronic Commerce . . .	271
14.3.2	Approach of the Commission of the European Community (CEC)	273
14.3.3	OECD Guidelines	275
14.3.4	Utah Digital Signature Act (1996)	276
14.3.5	German Digital Signature Act (1997)	277
14.3.6	Electronic Data Interchange Agreements	278
14.3.7	Conclusions	279
14.4	The <i>SEMPER</i> Electronic-Commerce Agreement	279
14.4.1	General	279
14.4.2	<i>SECA</i> CAs	280
14.4.3	<i>SECA</i> Legal Body	281
14.4.4	Joining <i>SECA</i>	281
14.4.5	Liability Limits in <i>SECA</i>	282
14.4.6	Blacklists of Players Claiming Compromised Keys and Signatures	284
14.4.7	Levels of Equipment	286
14.5	The Content of <i>SECA</i>	287
14.5.1	The Agreement	287
14.5.2	The Code of Conduct	292
14.5.3	The Guidelines	294
14.6	Conclusions	303
15.	Future Directions in Secure Electronic Commerce	305
15.1	Non-technical Issues	305
15.1.1	Security Awareness	305
15.1.2	Crypto Regulations	306
15.1.3	Legal Issues	307
15.2	Global Technical Issues	307
15.2.1	Process Orientation	307
15.2.2	Dispute Handling	308
15.2.3	Access Control	309
15.2.4	Pervasive Anonymity	310
15.2.5	Web Tracking, Personalized Accounts, and Directed Marketing	312
15.2.6	Multi-party Protocols	312
15.2.7	Visualization of Security	313
15.3	Services and Protocols	315
15.3.1	Business-Item Layer	315
15.3.2	Supporting Services	317
15.4	Implementation	320

15.4.1	Trusted Computing Base	320
15.4.2	Dependable Third-Party Implementations.....	321
15.4.3	Assurance	322
References		325
Glossary		335
Index		343