Gérard Lacoste Birgit Pfitzmann
Michael Steiner Michael Waidner (Eds.)

SEMPER – Secure Electronic Marketplace for Europe

Springer

Technische Universität Darmstadt
FACHBEREICH INFORMATIK
BIBLIOTHEK
Inventar-Nr.: I280-00314
Sachgebiete:
Standort:

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 *SEMPER* 13
      1.5.1 Security Requirements 13
      1.5.2 The *SEMPER* Focus 13

2. **Technical Framework** 15
   2.1 The *SEMPER* 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 *SEMPER* Electronic-Commerce Agreement 27
      3.3.1 Structure of *SECA* 27

3.3.2 Introducing Electronic-Commerce Agreements 28
3.4 Conclusions 29

4. **Vision of Future Products** 31
4.1 Four Facets of *SEMPER* as a Product 31
4.2 *SEMPER*-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 *SEMPER* 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 *SEMPER* 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 *SEMPER* 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 *SEMPER* 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 191
11.3.3 Design Overview 192
11.3.4 Purses 196
11.3.5 Transactions and Transaction Records 196
11.3.6 Payment Manager 197
11.4 Adapting a Payment System 198
11.5 Using the Generic Payment Service Framework 198
11.5.1 Payment Transactions 198
11.5.2 Special Application Functionality 199
11.6 Token-based Interface Definition 201
11.7 Extending the Design 203
11.7.1 Dispute Management 203
11.7.2 Payment Security Policies 206
11.8 Related Work 209
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 *SEMPER* 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 *SEMPER* Electronic-Commerce Agreement ... 279
14.4.1 General ... 279
14.4.2 *SECA* CAs ... 280
14.4.3 *SECA* Legal Body ... 281
14.4.4 Joining *SECA* ... 281
14.4.5 Liability Limits in *SECA* ... 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 *SECA* ... 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