

Lex Mercatoria: Electronic Commerce and Encryption Pages

Lex Mercatoria

copy @ www.lexmercatoria.org

Copyright © 2004 Lex Mercatoria

Contents

Lex Mercatoria: Electronic Commerce and Encryption Pages	1
Electronic Commerce Documents	1
Cryptography /Encryption	1
Agreements	2
Interest Groups	2
AES Algorithm (Advanced Encryption Standard)	3
Reference and Links	4
Security Software	5
Digital Signatures	9
Electronic Contracts and Electronic Commercial Documents	9
EDI - Electronic Data Interchange	10
Electronic Payments	11
Solutions	11
Discusion	12
Authentication Solutions - Virtual Identities	14
Government and other Documents: Stands/Approaches to Electronic Commerce	15
Cybercrime	16
Privacy	16
NoN-Privacy / Security?	16
Industry	17
Electronic Commerce Resource Sites	18
Metadata	20
SiSU Metadata, document information	20

Lex Mercatoria: Electronic Commerce and Encryption Pages

Electronic Commerce & Encryption

Electronic Commerce \046 Encryption Encryption

*Electronic Commerce Documents tiny UNCITRAL Model Law on Electronic Commerce (1996) > 3
<document manifest> ¹ < html, segmented text> < html, scroll, document in one> < pdf, landscape> 4
< pdf, portrait> < odf:odt, open document text> < plain text utf-8> < concordance> < dcc, document
content certificate (digests)> footnotesize tiny WTO Declaration on Global Electronic Commerce (Adopted 5
on 20 May 1998) > <document manifest> ² < html, segmented text> < html, scroll, document in
one> < pdf, landscape> < pdf, portrait> < odf:odt, open document text> < plain text utf-8> < con- 6
cordance> < dcc, document content certificate (digests)> footnotesize tiny OECD Recommendation of
the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce
(Organisation for Economic Co-operation and Development) 1999 > <document manifest> ³ < html,
segmented text> < html, scroll, document in one> < pdf, landscape> < pdf, portrait> < odf:odt, open
document text> < plain text utf-8> < concordance> < dcc, document content certificate (digests)> foot- 7
notesize tiny<Summary Of Electronic Commerce And Digital Signature Legislation> McBride
Baker & Coles !pick tiny<Technology-Neutral, Non-PKI, Minimalist E-Commerce Legisla- 8
tion> tiny<EFF "Privacy - Crypto - Export Restrictions, ITAR and EAR" Archive> Electronic 9
Frontier Foundation tiny<eCommerce & Legal issues> at <http://ecominfocenter.com/> eComIn- 10
foCenter.com tinyFor other documents related to electronic commerce (such as EDI or
cryptography) look under the relevant subject heading below. *Cryptography /Encryption 11
tinyThis list does not attempt to be exhaustive. It provides links to sources we have found
particularly useful, and to other more comprehensive lists of sources on the subject. tiny
Elsewhere off this site: <Electronic Commerce compendium> tinyCryptography applied in
various ways and circumstances is essential for security and trust: ParagraphIndent0mm

- confidentiality

- integrity

- authentication

- non-repudiation

In sum, read, cryptography impacts upon every aspect of considered e-commerce and private e-business relations.

#agreements Agreements

#groups Interest Groups

#aes AES Algorithm (Advanced Encryption Standard)

¹<http://www.jus.uio.no/lm/un.electronic.commerce.model.law.1996/sisu_manifest.html>

²<http://www.jus.uio.no/lm/wta.electronic.commerce.1998/sisu_manifest.html>

³<http://www.jus.uio.no/lm/oe.cd.consumer.protection.in.electronic.commerce.guideline.recommendation.1999/sisu_manifest.html>

#reference Reference	24
#software Security Software	25
⟨Crypto Law Survey⟩ ⟨Bert Jaap Koops⟩	26
⟨A Short History of Cryptography⟩ by Fred Cohen from ⟨Introductory Information Protection⟩ “a book about keeping people and organizations from harm caused by information. It requires little or mathematics and is suitable as a text for a graduate level or advanced undergraduate course.” Fred Cohen & Associates	27
⟨Why Cryptography Is Harder Than It Looks⟩ by Bruce Schneier CTO and Founder ⟨Coun- terpane Internet Security, Inc.⟩	28
Agreements	29
⟨Wassenaar Arrangement⟩	30
Interest Groups	31
⟨Center for Democracy and Technology⟩	32
⟨CryptoRights Foundation⟩	33
⟨Cyber Rights and Cyber Liberties UK⟩ on the ⟨Wassenaar Arrangement⟩ at ⟨Cyber Rights & Cyber Liberties⟩	34
⟨Electronic Frontier Foundation⟩	35
⟨International Cryptography Campaign⟩	36
⟨Foundation for Taxpayer and Consumer Rights⟩	37
⟨Global Internet Liberty Campaign⟩	38
⟨Free Congress Foundation⟩	39
⟨Echelonwatch⟩	40
⟨the American Civil Liberties Union⟩	41
⟨Electronic Frontiers Texas⟩	42
⟨Center for Media Education⟩	43
Industry	44
⟨Direct Marketing Association⟩	45
⟨TRUSTe⟩	46

AES Algorithm (Advanced Encryption Standard) 47

NIST AES 48

«AES Algorithm» Advanced Encryption Standard (AES) Development Effort, Computer Security Division, National Institute of Standards and Technology, NIST is an agency of the U.S. Commerce Department's Technology Administration see «Encryption toolkit» Advanced Encryption Standard of the National Institute of Standards and Technology (NIST) 49

«Report» 50

“SPECIAL NOTE - Intellectual Property NIST reminds all interested parties that the adoption of AES is being conducted as an open standards-setting activity. Specifically, NIST has requested that all interested parties identify to NIST any patents or inventions that may be required for the use of AES. NIST hereby gives public notice that it may seek redress under the antitrust laws of the United States against any party in the future who might seek to exercise patent rights against any user of AES that have not been disclosed to NIST in response to this request for information.” 51

«Information Technology Laboratory» 52

“Our goals are to strengthen the U.S. economy and improve the quality of life by providing the information technology industry and users with needed measurements and standards and to provide NIST with high quality information technology services.” 53

«Federal Information Processing Standards Publications» 54

«AES» entry on Wikipedia 55

AES Winner announced October 2nd, 2000 56

«Rijndael» by «Joan Daemen» and «Vincent Rijmen» « » of Belgium. 57

publications Vincent Rijmen «list» DBLP Bibliography Server «list» 2everything 58

Joan Daemen «list» DBLP Bibliography Server «list» 2everything 59

«Cryptix» 60

The Rijndael algorithm is based on a block cipher algorithm (The Block Cipher Square Algorithm) described in an article in the October, 1997 issue of DDJ « » 61

6{ 5 Finalists, August 1999 62

«Twofish» 63

«Rijndael» 64

«Serpent» 65

«MARS» 66

«RC6» 67

Data Encryption Standard (DES)	68
<Data Encryption Standard (DES)>	69
<Data Encryption Standard (DES), Triple DES, and Skipjack Algorithms>	70
<Triple DES Validation List>	71
<Overview Triple DES Encryption>	72
<Easy DES File Encryption Software for Organizations!>	73
<Strong Encryption Package> Federal Information Processing	74
<Announcing the Standard for Data Encryption Standard (DES)> FIPS PUB 46-2, Super-	75
sedes FIPS PUB 46-1, 1988 January 22 Federal Information Processing Standards Pub-	
lication 46-2 1993 December 30.	
Reference & Links	76
<The Crypto Link Farm - Encryption and Security-related Resources> A few of (the many)	77
mirrors auto-updated: < >	
<Security and Encryption-related Resources and Links> by Peter Gutmann	78
<Security pointers> by Tom Dunigan	79
<Security and Cryptography> by Mark McCutcheon	80
<Crypto - Cryptography resource on the Web> by Matt Blaze	81
<Cryptography and Security> <[+]> by <Ronald L. Rivest> <[+]>	82
<Crypto Page> Paulo Barreto	83
<Encryption and Security Tutorial>	84
<Cryptome>	85
<A Cryptographic Compendium> < > <alternative location>	86
<EFF "Privacy - Crypto - Export Restrictions, ITAR and EAR" Archive> Electronic Frontier	87
Foundation	
<Cryptography> Francis Litterio	88
<Security & Cryptography> <standards> by Michael Waidner	89
<Security and Encryption> <*> Quick Links	90
<Encryption and Security Tutorial>	91
<Encryption, Security & Privacy News> All E-Commerce	92
<Cryptographic Algorithms> <Mach5 Cryptography Archives>	93
<What's Hot in Encryption - Bulletins> EFF	94
<Cryptography: The Study of Encryption> <Cryptography> Francis Litterio	95
<How electronic encryption works and how it will change your business> <Viacorp . com>	96

<Security Encryption PGP>	97
<GPG - The GNU Privacy Guard> (Open PGP)	98
<The Linux Encryption-HOWTO Homepage> <Linux Encryption HOWTO> by Marc Mutz	99
<OpenPGP (RFC2440)>	100
<Snake Oil Warning Signs: Encryption Software to Avoid> an FAQ by Matt Curtin	101
<Mitre> CVE - Security Dictionary of Common Vulnerabilities and Exposures	102
<Counterpane>	103
<Infosyssec - Security Portal for Information System Security Professionals>	104

Security Software 105

Secure Point to Point Connection and File Sharing 106

<Open Secure Shell> - openSSH	107
<Linux FreeS/WAN> Secure point to point connection anywhere on the Internet, Strong Encryption. Developed outside the United States and not subject to US export restrictions.	108
<Linux PPTP Server> the PPTP Linux Server works with WinNT PPTP clients and C. S. Ananian's PPTP Linux clients. Virtual Private Networking technology enables the use the public Internet backbone for private data communications, encryption and encapsulation technology, permitting the carving out of a private channel/passageway through the Internet.	109
<Bizet> free download of V-ONE technology that permits secure connection with other users of the same technology. It performs authentication and uses 168-bit Triple DES encryption to secure e-commerce, as well as to encrypt data being transmitted as part of auctions, chat rooms, e-mail and classified advertisements. Adequate security has been a big obstacle to business-to-business commerce to date... July 1999	110
<Gnutella>	111
<Gnut> Linux/Unix console gnutella clone	112
<Freenet> (The Free Network Project Homepage) "Re-Wiring the Internet". Hosted by <Source Forge> "Freenet is a peer-to-peer network designed to allow the distribution of information over the Internet in an efficient manner, without fear of censorship. Freenet is completely decentralized, meaning that there is no person, computer, or organisation in control of Freenet or essential to its operation. This means that Freenet cannot be attacked like centralized peer-to-peer systems such as Napster. Freenet also employs intelligent routing and caching meaning that it learns to route requests more efficiently, automatically mirrors popular data, makes network flooding almost impossible, and moves data to where it is in greatest demand. All of this makes it much more efficient and scalable than systems such as Gnutella."	113

<Mojo Nation> claimed to be “a revolutionary new publishing and content-sharing network. [That]combines the flexibility of the marketplace and the distributed computing power of the Internet to go far beyond current filesharing systems... Mojo Nation is building an efficient, massively scalable and secure marketplace for distributors and consumers of digital content.” 114

<Wheres dot com> Internet file sharing programs 115

Encrypted Files and Mail 116

#linux Linux Solutions 117

#commercial Commercial 118

<UP - Ultimate Privacy> 119

<Speak Freely> 120

<Speak Free> Secure fully encrypted Chat Program 121

<Speak Freely Unix> <Windows> 122

<HushMail> web based secure e-mail 123

<Freedom> “Untraceable” privacy system from ZeroKnowledge 124

<1on1 Secure Mail> The free-to-use service that requires the use of a sizable e-mail Windows PC client, which may be downloaded from the site or obtained on CD. 125

<Mutt> a pgp-aware mailer 126

<SUIDNet> “secure IRC network” 127

<The International PGP Page> 128

<Top level home page for www.pgp.net> 129

<GPG - GNU Privacy Guard> <Download GPG> which uses only free algorithms, and conforming to the OpenPGP standard 130

<OpenPGP (RFC2440)> 131

PGP Sites <#fix> 132

<PGP DH v RSA FAQ> 133

Linux Encryption Solutions 134

See also <Linux Encryption> 135

<GPG - GNU Privacy Guard> <Download GPG> which uses only free algorithms, and conforming to the OpenPGP standard 136

<Project Aegypten (Free Software Sphinx-Clients)> for Linux “The Sphinx project launched by German authorities aims to improve secure email exchange... Proprietary products are already on the way, but with the project ?gypten there is now also a Free Software 137

solution going to be realized for popular mail user agents (sphinx-enabling KMail and mutt are essential goals).”

- ⟨SuSE Linux (since v7.2) provides a Secure Crypto File System based on Twofish⟩ 138
- ⟨The Linux Encryption-HOWTO Homepage⟩ ⟨Linux Encryption HOWTO⟩ by Marc Mutz 139
 - ⟨Encrypting Disks⟩ 140
 - ⟨Encrypting your Disks with Linux⟩ Doobee. R. Tzeck 141
 - ⟨PPDD⟩ requires recompiling (patching) the Linux kernel to allow strong encryption and a special device. Good documentation. 142
 - ⟨TCFS⟩ involves the running of a daemon which exports an encrypted filesystem as an NFS share. 143
 - ⟨Crypto Kernel Patch⟩ a patch for any given Linux kernel to make the loopback device use encryption algorithms. 144
 - ⟨BestCrypt⟩ ⟨Jetico⟩ 145

Steganography

- ⟨Steghide⟩ 146
- ⟨Outguess⟩ Steganography 147
- ⟨StegFS - A Steganographic File System for Linux⟩ 149

Organizations

- ⟨Internet Engineering Task Force⟩ 151
- ⟨IEEE Computer Society⟩ 152
- ⟨International Association for Cryptography Research⟩ 153
- ⟨National Security Agency⟩ U.S.A. 154
- ⟨National Institute of Standards and Technology⟩ NIST is an agency of the U.S. Commerce Department's Technology Administration 155
- ⟨NCSA⟩ 156
- ⟨DSS Defense Security Service⟩ 157
- ⟨National Infrastructure Protection⟩ U.S. Department of Homeland Security 158
- ⟨The Critical Infrastructure Assurance Office (CIAO)⟩ moved to the U.S. Department of Homeland Security 159
- ⟨ANSI - American National Standards Institute⟩ 160
- ⟨National Information Assurance Partnership⟩ 161
- ⟨Office of Information Security⟩ 162
- ⟨International Telecommunication Union⟩ 163

‹Internet Security Alliance‹ a non-profit collaboration between EIA and Carnegie Mellon's CERT Coordination Center (CERT/CC), with a diverse and international membership	164
‹ETSI‹ Telecom Standards	165
‹SET Secure Electronic Transactions‹	166
‹Association for Computing Machinery‹	167
‹SANS Institute‹	168
‹CSI - Computer Security Institute‹	169
‹TruSecure‹	170
‹CERT‹ a center of Internet security expertise	171
‹ ‹	172
Commercial	173
‹RSA Data Security‹ ‹RSA‹	174
‹RSA Security‹ “the most trusted name in e-security”	175
RSA Security Incorporated owned key encryption patents (US) which expired September 26 th 2000.	176
‹Baltimore Security‹	177
Other	178
‹UP - Ultimate Privacy‹	179
‹VeriSign‹	180
‹Speak Freely‹	181
‹Speak Free‹ Secure fully encrypted Chat Program	182
‹Speak Freely Unix‹ ‹Windows‹	183
‹Crypto-Central SHA algorithm MD5 etc.‹ Delphi: Advanced encryption Components	184
Biometrics	185
‹The Biometric Consortium‹	186
‹The International Biometric Society‹	187
‹Biometrics‹ A Journal of the International Biometric Society	188
‹Biometric Consortium‹	189
‹Biometrics‹	190
‹Biometric Encryption information‹	191
‹The Bio API‹	192
‹VeriSign‹	193

Quantum physics cryptography	194
<NTT>	195
<Almaden Research Lab>	196
<Los Alamos>	197
<British Telecom>	198
Digital Signatures	199
This list does not attempt to be exhaustive. It provides links to sources we have found particularly useful, and to other more comprehensive lists of sources on the subject.	200
Elsewhere off this site: <Electronic Commerce compendium>	201
<UNCITRAL Model Law on Electronic Signatures (2001)>	202
Electronic Signatures in Global and National Commerce Act, 2000, United States	203
is law, granting (from 1 st October, 2000) electronic signatures the same binding legal status as hand-written signatures and thereby making the signing of enforceable contracts online possible on the click of a mouse, with all that that may imply.	204
<Bill>	205
“A bill to regulate interstate commerce by electronic means by permitting and encouraging the continued expansion of electronic commerce through the operation of free market forces, and for other purposes”	206
<Interdisciplinary Centre for Law & Information Technology, ICRI>	207
<Legal Aspects of the E-Revolution> <(archived site)> European Commission - Information Society Directorate-General	208
<Internet Law & Policy Forum> “dedicated to promoting the global growth of e-commerce by contributing to a better understanding of the particular legal issues which arise from the cross border nature of the electronic medium”	209
<Links on Law, Cryptography and Electronic Communications> Prepared by Juan A. Avellan of the Information Technology Law Unit, Queen Mary and Westfield College	210
<Law Center on Electronic Signatures>	211
<Global E-Commerce Law> Baker & McKenzie	212
<The CyberNotary Committee> Science and Technology Section of the American Bar Association co Chairs: Theodore S. Barassi & Joseph H. Alhadeff	213
<Digital Notary Systems> American Bar Association	214
<Digital Signatures Guidelines> American Bar Association	215

Electronic Contracts and Electronic Commercial Documents 216

This list does not attempt to be exhaustive. It provides links to sources we have found 217

particularly useful, and to other more comprehensive lists of sources on the subject.	
Elsewhere off this site: <Electronic Commerce compendium>	218
<ebXML> The UN and OASIS effort: "Creating a Single Global Electronic Market"	219
<Monthly Archives for ebxml-awareness>	220
<Electronic Business XML Initiative (ebXML)> The XML Cover Pages by Robin Cover	221
< >	
<XAML> (Transaction Authority Markup Language) "vendor neutral that enables the co-ordination and processing of online transactions in the rapidly developing in the rapidly emerging world of XML web services" backed by Hewlet Packard, IBM, Oracle, and Sun.	222
<XAML Cover Page> <FAQ>	
<Bolero> <*>	223
Bolero backed by about 120 banks and logistics firms is trying to set up a global standard that would be accepted by governments, shippers, and banks. In doing so the plan to tackle such age old legal concepts as the bill of lading. Bolero plans to use an encrypted communication network to shuffle documents around the world, a process that's now hampered by incompatible computer systems and bureaucrats. Bolero is owned 50-50 by the	224
<eOriginal> Electronic Original (Steven Bisbee). From 1999	225
"eOriginal, Inc. has developed and markets, under two U.S. patents, a fully integrated transaction system that delivers the trusted means for producing electronic documents that are unique, secure and reliable for all business and legal purposes. The company's product suite, marketed as eOriginal, enables the creation of the Electronic Original."	226
EDI - Electronic Data Interchange	227
This list does not attempt to be exhaustive. It provides links to sources we have found particularly useful, and to other more comprehensive lists of sources on the subject.	228
Elsewhere off this site: <Electronic Commerce compendium>	229
<Electronic Commerce and EDI> at NRCCL's Law and Information Technology Links Norwegian Research Center for Computers and Law <NRCCL>	230
check UNECE for the United Nations/EDIFACT Standards.	231
Revised articles of draft uniform rules on the legal aspects of electronic data interchange	232
United Nations Revised draft model statutory provisions on the legal aspects of electronic data interchange	233
<X12 Transaction Set Index Version 3040>	234
<Harbinger> Now holds Premonos materials	235
<UNeTradeS.net>	236

◁Electronic Commerce & Electronic Data Interchange: Internet Resources▷ Golden Gate University Library Guide 237

Electronic Payments 238

Elsewhere off this site: ◁Electronic Commerce compendium▷ 239

Solutions 240

◁NACHA - Electronic Payments Association▷ “NACHA is a not-for-profit trade association that develops operating rules and business practices for the Automated Clearing House (ACH) Network and for other areas of electronic payments. ? NACHA activities and initiatives facilitate the adoption of electronic payments in the areas of Internet commerce, electronic bill payment and presentment (EBPP), financial electronic data interchange (EDI), international payments, electronic checks, electronic benefits transfer (EBT) and student lending. We also promote the use of electronic payment products and services, such as Direct Deposit and Direct Payment. 241

NACHA represents more than 12,000 financial institutions through our network of regional ACH associations.? We have over 600 members in our seven industry councils and corporate Affiliate Membership program.” 242

◁Internet Council - NACHA▷ 243

◁Project ACTION▷ “a program to develop a payment product for Internet transactions utilizing Automated Clearing House (ACH) credits” 244

◁E-Cash Technologies Inc.▷ “global software solutions that extend and enhance physical-world payment methods” 245

◁Cybercash▷ “VeriSign and CyberCash join forces to offer complete e-commerce solutions” 246

◁Globeset Trinitech▷ “securing payment in the digital age” 247

◁Mobey Forum▷ “a financial industry-driven forum, whose mission is to encourage the use of mobile technology in financial services ... - such as payment, remote banking and brokerage” 248

◁Paypal▷ Confinity. Paypal now Nokia approved allows you to make instant payments to anyone with a cell phone, two-way pager, or handheld device, such as the Palm? organizer. Permits such things as the settlement of debts, borrowing of cash and splitting of bills/ expenses without the hassle of going to ATMs or keeping track of debts. Paypal is free and works seamlessly with your existing credit card and bank account. PayPal? software can be “beamed” to your friend or business associate who can then be “beamed” money instantly. The system charges your credit card when you next sync your device, and your friend can register later at PayPal.com. 249

◁E-Commerce Guide▷ 250

⟨BigStep⟩ Build your own web-based e-commerce site, free service	251
⟨ECML⟩ Electronic Commerce Modeling Language (ECML) is to be a universal format for wallets and merchant web sites. ECML uses a set of uniform field names to streamlines the process by which merchants collect electronic data for shipping, billing, and payment. Its development is a collaboration between: American Express, AOL, Compaq, CyberCash, IBM, MasterCard, Microsoft, SETCo, Sun Microsystems, Transactor Networks, Trintech, and Visa. 18/06/1999	252
⟨FpML⟩ FpML, an XML-based markup language that allows for Net-based integration of services such as electronic trading and risk analysis backed by IBM, PricewaterhouseCoopers and J.P. Morgan. 18/06/1999	253
⟨WorldPay⟩	254
⟨NetBanx⟩	255
⟨Payment mechanisms designed for the Internet⟩ by Michael Peirce	256
⟨Digital Money, Credit Cards, and Electronic Payment Systems⟩	257
⟨Page of links to resources on Electronic Money or E-Money⟩ by Roy Davies.	258
⟨DigiCash (went under)⟩ ⟨Electronic Money (That's What I Want)⟩ (Read up on David Chaum) Article by Steven Levy for HotWired, December 1994. ⟨David Chaum Publications⟩ ⟨How much do you trust Big Brother?⟩ interview of David Chaum, 1997 & the ⟨Mark Twain Bank⟩	259
⟨CyberCash⟩	260
⟨CheckFree⟩ “the undisputed leader in moving money electronically”	261
⟨VeriFone⟩	262
⟨Millicent⟩ (Digital / Compaq)	263
⟨Open Market⟩	264
⟨MasterCard⟩	265
⟨Visa⟩	266
⟨Hyper Mart⟩ free service with advertising part of the Go2Net network	267
⟨Sitematic⟩ monthly charges	268
⟨MindSpring Biz⟩ monthly charges	269
⟨MS Solutions for small businesses⟩	270
E-Commerce servers	271
Discussion	272
This list does not attempt to be exhaustive. It provides links to sources we have found particularly useful, and to other more comprehensive lists of sources on the subject.	273
Elsewhere off this site: ⟨Electronic Commerce compendium⟩	274

⟨W3C - Electronic Commerce Interest Group?⟩ W3C has closed its Ecommerce and Micropayment Activity, but through a number of activities W3C is committed to key factors for success in the evolution of Electronic Commerce.	275
⟨Guide to Online Payments⟩ US Federal Trade Commission	276
⟨NACHA - Electronic Payments Association⟩ NACHA is a not-for-profit trade association that develops operating rules and business practices for the Automated Clearing House (ACH) Network and for other areas of electronic payments. NACHA represents more than 12,000 financial institutions through our network of regional ACH associations.? We have over 600 members in our seven industry councils and corporate Affiliate Membership program.?	277
⟨Electronic Payments Forum⟩	278
⟨Electronic Money, or E-Money, and Digital Cash⟩ links by Roy Davies	279
⟨Epayment Links⟩ Institute for eCommerce, Carnegie Mellon University	280
⟨Electronic Commerce, Payment Systems, and Security⟩ links by Michael Waidner	281
⟨Internet Funds Transfer Services - Electronic Payments⟩ Elsop - Electronic Software Publishing Corporation	282
⟨A Bibliography of Electronic Payment Information⟩	283
⟨Links related to Smart Cards and Electronic Payment Systems⟩	284
⟨Payment Systems Information Resources⟩ Federal Reserve Bank of New York	285
⟨United States Government Electronic Commerce Policy⟩	286
⟨European ePayments Observatory⟩	287
⟨The Future of Money⟩ edited by Robert Knautz, 1997 Policy Spotlight	288
⟨Payment mechanisms designed for the Internet⟩ by Michael Peirce	289
⟨Epayment Solutions - page sponsored by IBM⟩	290
Joint Electronic Payments Protocol (JEPI) to make it easier for consumers to use multiple payment systems from Web browsers:	291
⟨World Wide Web Consortium⟩	292
⟨CommerceNet⟩	293
⟨Millicent⟩ from Digital Equipment Corporation ⟨Information⟩	294
Microsoft: ⟨Passport⟩	295
⟨Electronic Money / Internet Payment Systems⟩	296
⟨Network Payment Mechanisms and Digital Cash by Michael Peirce⟩	297
⟨Central Banking Resource Center⟩ Mark Bernkopf	298
⟨e\$ Page⟩ Robert Hettinga	299
⟨Debt, Money and Ancient Meme⟩	300
⟨21 st Century Banking Alert Page⟩ also ⟨Additional Online Resources⟩ and ⟨BancMail	301

Archive› at ‹Fried, Frank, Harris, Shriver and Jacobson›
‹A Bibliography of Electronic Payment Information› 302

Writings and Links to them 303

‹E-Commerce Times› News 304

‹A Bibliography of Electronic Payment Systems› 305

‹Alternative Money Systems› ‹New Civilization Network› 306

‹Money - Past, Present & Future› Sources of Information on Monetary History, Contemporary Developments, and the Prospects for Electronic Money maintained by Roy Davies 307

‹The Future of Money in the Information Age› by the Cato Institute, 1997. 308

‹The Surprise Weapon: Private Enterprise Money› by E. C. Riegel, 1944. 309

‹Array› including the ‹Journal of Internet Banking and Commerce› and ‹Journal of Internet Purchasing› 310

‹The Surprise Weapon: Private Enterprise Money› by E. C. Riegel, 1944. 311

‹Implications for Central Banks of the Development of Electronic Money› 11th November 1996 by the ‹Central Banker's Central Bank› the Bank for International Settlement, Basle, Switzerland. 312

‹Crypto-Anarchy and Virtual Communities› by Timothy C. May (1995) 313

Commerce Related Sites including ‹Banking› and ‹Finance› 314

Authentication Solutions - Virtual Identities 315

‹Liberty Alliance Project› (Sun etc.) 316

‹Passport› ‹Passport, Hailstorm, .Net etc.› Microsoft 317

 ‹Oblix | Identity-Based Security Solutions(TM)› 318

‹The DotGNU Project› 319

‹Linux-PAM› “Pluggable Authentication Modules for Linux is a suite of shared libraries that enable the local system administrator to choose how applications authenticate users.” 320

‹PAM - Pluggable Authentication Modules› 321

‹documentation for Linux-PAM› 322

‹PAM - FAQ› 323

‹PAM› 324

‹User Authentication HOWTO› “Explains how user and group information is stored and how users are authenticated on a Linux system (PAM), and how to secure your system's user authentication.” by Peter Hernberg 325

Government and other Documents: Stands/Approaches to Electronic Commerce	326
This list does not attempt to be exhaustive. It provides links to sources we have found particularly useful, and to other more comprehensive lists of sources on the subject.	327
Elsewhere off this site: <Electronic Commerce compendium>	328
<Electronic commerce in the WTO>	329
<Electronic Commerce> at the International Chamber of Commerce	330
<United States Government Electronic Commerce Policy>	331
<International Sites>	332
<A Framework for Global Electronic Commerce>	333
<A Framework For Global Electronic Commerce>	334
<W3C Activities Related to the US "Framework for Global Electronic Commerce">	335
<Electronic Commerce and the European Union>	336
<Legal Aspects of the E-Revolution> European Commission - Information Society Directorate-General	337
<WTO's work programme on electronic commerce>	338
<Electronic Commerce and the European Union> <ECLIP>	339
<EU Initiative in Electronic Commerce> 1997	340
<Wassenaar Arrangement>	341
<Ecommerce> at the <Global Information Infrastructure Commission> of the <Center for Strategic & International Studies>	342
This group backed "The Commerce Standard", described as: a uniform open and free standard for Electronic Commerce. ZiffDavis publisher initiative developed collaboratively with more than 200 top global Internet merchants, IT vendors, analysts, policymakers, consumer advocates, academics and journalists in an effort to establish a set of merchant practices and policies. Topics for Draft 1.0 include: merchant information, product availability, charges and fee information, warranties, product support, search capabilities, privacy, security, payment and billing, receipt of order notification, order status and history, shipping delivery and order execution, cancellations, returns, refunds and customer support. Launched in 12 July 1999, completion planned for December 1999. Global Information Infrastructure.	343
<Global Business Dialogue on Electronic Commerce> <(GBDe)> An international non-governmental organization, managed by executives of 29 major enterprises in the United States, Europe and Asia, that promotes establishing global rules for electronic commerce over the Internet.	344
GBDe member companies submit requests for legal arrangements for electronic commerce representing the interest of industries during the first GBDe convention	345

held on 13 September 1999 in Paris, and these will be submitted to the government of each country.

The following nine themes will be covered: (1) authentication and security, (2) consumer credibility, (3) contents/business communication, (4) inter-operability of information infrastructure and governance, (5) intellectual property, (6) control, (7) reliability, (8) protection of private data and (9) taxes/tariffs. 346

Member companies include: Japan - Fujitsu Ltd., NEC Corp., Toshiba Corp., Mitsui & Co., Ltd., Mitsubishi Bank Ltd., Nippon Telegraph and Telephone Corp; North America - IBM Corp., MCIWorldcom Inc., Nortel Networks Corp., Time Warner Inc. and Walt Disney Co.; Europe - France Telecom, Nokia of Finland, DaimlerChrysler Corp. of Germany and others. 347

Cybercrime 348

⟨Convention on Cybercrime⟩ Budapest, 2001, Council of Europe 349

⟨Other COE Pages related to the Convention on Cybercrime⟩ 350

⟨Draft Convention on Cyber-crime (Draft N? 19)⟩ politechbot 351

Privacy 352

See also ⟨Linux Encryption⟩ 353

⟨Electronic Privacy Information Center⟩ 354

⟨P3P⟩ WWW Consortium 355

⟨Encryption, Security & Privacy News⟩ All E-Commerce 356

⟨What's Hot in Encryption - Bulletins⟩ EFF 357

⟨GPG - The GNU Privacy Guard⟩ (Open PGP) 358

⟨Privacy Foundation⟩ 359

NoN-Privacy / Security? 360

⟨Echelon Watch⟩ administered by ACLU (American Civil Liberties Union) in conjunction with the Free Congress Foundation, the Electronic Privacy Information Center, Cyber-Rights and Cyber-Liberties (UK) and the Omega Foundation. 361

⟨Echelon Watch⟩ Cyber-Rights & Cyber-Liberties (UK) 362

⟨Statewatch⟩ monitoring the state and civil liberties in the European Union 363

Interest Groups & Campaigns

364

Interest Groups \046 Campaigns Campaigns\0mm

364tinyThis list does not attempt to be exhaustive. It provides links to sources we have found particularly useful, and to other more comprehensive lists of sources on the subject. tinyElsewhere off this site: <Electronic Commerce compendium> tiny<Wassenaar Arrangement> tiny<Center for Democracy and Technology> tiny<Center for Media Education> tiny <Cyber Rights and Cyber Liberties U.K> a non-profit civil liberties organisation founded by Yaman Akdeniz. Information on <Wassenaar> and on the UK <Freedom of information Files> tiny<Distributed.Net> tiny<Electronic Freedom Frontier> tiny<Electronic Frontier Foundation> tiny<Electronic Privacy Information Center> tiny<EU Freedom Campaign*> tiny<Foundation for Taxpayer and Consumer Rights> tiny<CryptoRights Foundation> tiny<Global Internet Liberty Campaign> tiny<International Cryptography Campaign> tiny<Echelonwatch> tiny<The Internet Law and Policy Forum> “dedicated to promoting global growth of e-commerce by contributing to a better understanding of the particular legal issues which arise from the cross border nature of the electronic medium” tiny<Free Congress Foundation> tiny <the American Civil Liberties Union> tiny<Center for Media Education> tiny<Security Forum> *Industry tiny<Direct Marketing Association> tiny<Interactive Services Association> tiny<TRUSTe> tiny<Global Information Infrastructure Commission> This group backed “The Standard for Internet Commerce”, described as: a uniform open and free standard for Electronic Commerce. ZiffDavis publisher initiative developed collaboratively with more than 200 top global Internet merchants, IT vendors, analysts, policymakers, consumer advocates, academics and journalists in an effort to establish a set of merchant practices and policies. Topics for Draft 1.0 include: merchant information, product availability, charges and fee information, warranties, product support, search capabilities, privacy, security, payment and billing, receipt of order notification, order status and history, shipping delivery and order execution, cancellations, returns, refunds and customer support. Launched in 12 July 1999, completion planned for December 1999. Global Information Infrastructure. tiny<Global Business Dialogue on Electronic Commerce> <(GBDe)> An international non-governmental organization, managed by executives of 29 major enterprises in the United States, Europe and Asia, that promotes establishing global rules for electronic commerce over the Internet. ParagraphIndent0mmGBDe member companies submit requests for legal arrangements for electronic commerce representing the interest of industries during the first GBDe convention held on 13 September 1999 in Paris, and these will be submitted to the government of each country.

365

366

367

368

369

370

371

372

373

The following nine themes will be covered: (1) authentication and security, (2) consumer credibility, (3) contents/business communication, (4) inter-operability of information infrastructure and governance, (5) intellectual property, (6) control, (7) reliability, (8) protection of private data and (9) taxes/tariffs.

393

Member companies include: Japan - Fujitsu Ltd., NEC Corp., Toshiba Corp., Mit-

394

sui & Co., Ltd., Mitsubishi Bank Ltd., Nippon Telegraph and Telephone Corp; North America - IBM Corp., MCIWorldcom Inc., Nortel Networks Corp., Time Warner Inc. and Walt Disney Co.; Europe - France Telecom, Nokia of Finland, DaimlerChrysler Corp. of Germany and others.

Electronic Commerce Resource Sites	395
<eComInfoCenter.com>	396
<Summary Of Electronic Commerce And Digital Signature Legislation> McBride Baker & Coles !pick	397
<E-Business Research Center> CIO	398
<E-Commerce> Follesdal, Coolconnect (check details)	399
<Technology-Neutral, Non-PKI, Minimalist E-Commerce Legislation>	400
<E-Commerce News Archive>	401
<Electronic Commerce and EDI> NRCCL's Law and Information Technology Links	402
<E-Commerce Project> America Online	403
<Electronic Commerce> by Michael Waidner	404
<Electronic Commerce Online Resources> List maintained by Gilbert & Tobin, Australia	405
<Electronic commerce section of the WTO website>	406
<WTO's work programme on electronic commerce>	407
<Electronic Commerce> at the International Chamber of Commerce	408
<US Government Ecommerce Policy>	409
<Ecommerce> at the <Global Information Infrastructure Commission> of the <Center for Strategic & International Studies>	410
<Electronic Commerce> Morino Institute	411
<Electronic Commerce and the European Union>	412
<European Internet Forum> (including Globalisation and the Information Society; Digital signatures and encryption; Internet Governance)	413
<DTI ECommerce> UK Department of Trade and Industry	414
<DTI E-Commerce Directive>	415
<Communications and information industries>	416
<Electronic Commerce Library> American Bar Association: "a research project funded by the European Commission's DG XIII, which seeks to set up a platform on the legal issues of electronic commerce with the objective of providing legal support to EC-funded RTD projects on any issue of law linked to electronic commerce, thereby stimulating expertise and increasing general awareness of the existing or recommended legal framework of electronic commerce."	417

- ◁E-Comm Links▷ E-Commerce Task Force, Canada 418
- ◁Center for Law, Commerce and Technology▷ School of Law University of Washington 419
- ◁Electronic Frontiers Australia▷ “representing Internet users concerned with on-line freedoms” 420
- ◁The Commerce Standard▷ The Standard for Internet Commerce is a uniform open and free standard for Electronic Commerce. ZiffDavis publisher initiative developed collaboratively with more than 200 top global Internet merchants, IT vendors, analysts, policymakers, consumer advocates, academics and journalists in an effort to establish a set of merchant practices and policies. Topics for Draft 1.0 include: merchant information, product availability, charges and fee information, warranties, product support, search capabilities, privacy, security, payment and billing, receipt of order notification, order status and history, shipping delivery and order execution, cancellations, returns, refunds and customer support. Launched in 12 July 1999, completion planned for December 1999. Global Information Infrastructure. 421
- ◁Global Business Dialogue on Electronic Commerce▷ ◁(GBDe)▷ An international non-governmental organization, managed by executives of 29 major enterprises in the United States, Europe and Asia, that promotes establishing global rules for electronic commerce over the Internet. 422
- GBDe member companies submit requests for legal arrangements for electronic commerce representing the interest of industries during the first GBDe convention held on 13 September 1999 in Paris, and these will be submitted to the government of each country. 423
- The following nine themes will be covered: (1) authentication and security, (2) consumer credibility, (3) contents/business communication, (4) inter-operability of information infrastructure and governance, (5) intellectual property, (6) control, (7) reliability, (8) protection of private data and (9) taxes/tariffs. 424
- Member companies include: Japan - Fujitsu Ltd., NEC Corp., Toshiba Corp., Mitsui & Co., Ltd., Mitsubishi Bank Ltd., Nippon Telegraph and Telephone Corp; North America - IBM Corp., MCIWorldcom Inc., Nortel Networks Corp., Time Warner Inc. and Walt Disney Co.; Europe - France Telecom, Nokia of Finland, DaimlerChrysler Corp. of Germany and others. 425
- ◁Guidelines of the Electronic Commerce and Consumer Protection Group▷ [the “Group” appears to be gone] (America Online, AT&T, Dell Computer Group, IBM, Microsoft, Network Solutions, Time Warner Inc., Visa USA Inc) 426

Metadata

SiSU Metadata, document information

Document Manifest @:

<http://www.jus.uio.no/lm/electronic.commerce/sisu_manifest.html>

Title: Lex Mercatoria: Electronic Commerce and Encryption Pages

Creator: Lex Mercatoria

Rights: Copyright (C) 2004 Lex Mercatoria

Subject: electronic commerce, encryption

Publisher: SiSU <<http://www.jus.uio.no/sisu>> (this copy)

Date: 2004

Topics Registered: navigation:electronic commerce

Version Information

Sourcefile: electronic.commerce.sst

Filetype: SiSU text 2.0

Source Digest: SHA256(electronic.commerce.sst)=ccfe617ec8b817852135ed4ec5760872ec0c341a3624ea2b08b8f177351198cd-

Skin Digest: SHA256(skin_lm_nav.rb)=87fe13748e3cbcb0dedea211464f31bb26b0b111fd877b18f1812e06ec059cd5

Generated

Document (dal) last generated: Tue Sep 21 16:44:59 -0400 2010

Generated by: SiSU 2.6.3 of 2010w30/3 (2010-07-28)

Ruby version: ruby 1.8.7 (2010-08-16 patchlevel 302) [i486-linux]