Index

A
A P3P Preference Exchange Language (APPEL) 176
access control 80
access control mechanisms 34
accountability, pseudonym technology 142
action 211
active attacks 87
adware 131
AHIMA (American Health Information Management Association) 58
anonymity 119
anonymity, pseudonym technology 142
anti-virus software 117
APIs (application programming interfaces) 177
assertion 227
AT&T Privacy Bird 3
attribute assertion 227
audit trails 78
authentication 227
authentication assertion 227
authentication decision assertion 227
authenticity 209
authorization decision request 211, 213
authorization decision response 222, 224

B
backdoors 126
biometric systems 79
biometrics 84
blind signature 149
Bugnosis 16

C
CA (certification authority) 144
Canadian Standards Association (CSA) 4, 236
careless disclosure safeguards 81
CIA (confidentiality, integrity, and availability) 121
Code of Fair Information Practices 4
Common Criteria 194
Computer Security Institute (CSI) 67
CONFAB 239
confidentiality 209
consent 229
cost 2
cookies 9, 123
credential 150
cryptography 83, 209
cryptography, XML 209
CSA Model Code  2

cyberspace  142

D
DAC (discretionary access control)  81
DAFMA T (Dynamic Authorization Framework for Multiple Authorization Types)  180
DAML-S  40
data aggregation  6
data controllers  257,  286
data processor  257,  286
data profiling  6
data subject  257,  287
database management systems (DBMS)  46
database security  81
decision process  2
decryption  148
decryption keys  35
decryptor  157
demilitarized zone (DMZ)  49
digital pseudonym  143
digital rights management (DRM)  10,  192,
                               239
digital signature  209
discretionary access control (DAC)  81
domain-type enforcement (DTE)  180
duty of confidentiality  2

E
ecash (electronic cash)  153
e-coin  161
e-health database application  32
E-Marketplace UDDI Registry  50
e-services  204,  235,  281,  282
e-ticket  144,  155
e-voting  144,  156
e-wallet  144
ECHR  286
electronic cash (e-cash)  153
electronic commerce  3
electronic communication services  61
cryptographic  76,  209
cryptographic algorithms  35
time-based access control (TBAC)  81

Enterprise Privacy Authorization Language (EPAL)  15,  38,  176
environment  211
environmental threats  124
Europe Union Data Protection Directive  30
European Convention of Human Rights and Fundamental Freedoms (ECHR)  286
European Privacy Directive (95/46/EC)  4
exposure  2
eXtensible Access Control Markup Language (XACML)  177,  204,  213
eXtensible Markup Language (XML)  206,
                               229,  235
eXtensible Stylesheet Language Transformation (XSLT)  185

F
feature interactions  266
Federal Trade Commission (FTC)  30
Firewalls  49,  78,  83,  117

G
Goal-oriented Requirements Language (GRL)  269
GUI  248

H
hackers  67,  116
hash functions  36
health information  57
Health Insurance Portability and Account-
ability Act (HIPAA)  30,  145,  289
Healthcare Finance Administration (HCFA)  74
healthcare industry  57
healthcare privacy  57
healthcare professionals  57
Hippocratic database  179
hird-party cookie  9
human computer interaction (HCI)  14
human errors  66
human threats  124
IBM’s Enterprise Privacy Architecture (EPA) 239
identity and access management 205, 222
identity based encryption (IBE) 181
incentives 2
information privacy 30
information technology 57
informed consent 6
integrity 209
inter-organizational privacy enforcement engine (IOPP) 187
Internal Enterprise Application UDDI Registry 49
Internet 57
Internet privacy 3
intrusion detection monitoring 78
intrusion detection systems 133
IPSec (IPSec) 77
jurisdiction 231
Legislation 231
Liberty Alliance ID-Web Services Framework 239
local privacy enforcement engine (LPEE) 187
local privacy policy (LPP) 188
malicious software 124
malware 122
management infrastructure 240
medical record 57, 204
multi-attribute utility theory 4
multi-issue automated negotiation 4
namespaces 207
natural threats 124
negotiation strategy 4
non-functional requirements 268
obligation 211
omnivore 17
operating system 129, 133
Organization for the Advancement of Structured Information Standards (OASIS) 196
organization policies 236
organizational privacy enforcement engine (OPPE) 187
organizational privacy policy (OPP) 189
OWL Web Ontology Language 40
P3P (see Platform for Privacy Preferences Project)
Partner Catalog UDDI Registry 50
passive attacks 87
password management 80
patient databases 62
patients 56, 57
penetration testing 135
personal digital assistants (PDAs) 87
Personal Health Information Protection Act (PHIPA) of 2004 30
personal information (PI) 242
Personal Information Protection and Electronic Documents Act (PIPEDA) 30, 145, 184, 282
personal privacy policies 181
personally identifiable information (PII) 186
personally identifiable information tracking data 256
phishing 121, 126, 135
physicians 57
Platform for Privacy Preferences Project (P3P) 3, 36, 173, 231, 277
policies 204
policy decision point (PDP) 205
policy definition languages 173
policy enforcement point (PEP) 205
policy information points (PIPs) 205
policy sets 213
Portal UDDI Registry 49
privacy 30, 115
### Index 303

<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>privacy (impact) assessment</td>
<td>267</td>
</tr>
<tr>
<td>Privacy Act of 1974</td>
<td>30</td>
</tr>
<tr>
<td>privacy architecture</td>
<td>234</td>
</tr>
<tr>
<td>Privacy Commissioner</td>
<td>12</td>
</tr>
<tr>
<td>privacy enforcement</td>
<td>173, 182</td>
</tr>
<tr>
<td>privacy enhancing technologies (PETs)</td>
<td>173</td>
</tr>
<tr>
<td>privacy impact assessment (PIA)</td>
<td>15</td>
</tr>
<tr>
<td>Privacy Incorporated Software Agents</td>
<td>14</td>
</tr>
<tr>
<td>project (PISA)</td>
<td></td>
</tr>
<tr>
<td>privacy management</td>
<td>2</td>
</tr>
<tr>
<td>privacy policies</td>
<td>3, 30, 204</td>
</tr>
<tr>
<td>privacy policy architecture (PPA)</td>
<td>186</td>
</tr>
<tr>
<td>privacy policy compliance system (PPCS)</td>
<td>249</td>
</tr>
<tr>
<td>privacy principles</td>
<td>239, 285</td>
</tr>
<tr>
<td>privacy protection</td>
<td>142</td>
</tr>
<tr>
<td>privacy protection principles</td>
<td>267</td>
</tr>
<tr>
<td>privacy requirements</td>
<td>244</td>
</tr>
<tr>
<td>privacy rights management (PRM)</td>
<td>10, 255</td>
</tr>
<tr>
<td>privacy risks</td>
<td>2</td>
</tr>
<tr>
<td>Privacy Seal programs</td>
<td>194</td>
</tr>
<tr>
<td>privacy-aware role-based access control</td>
<td>(PARBAC) 180</td>
</tr>
<tr>
<td>PrivacyPact protocol</td>
<td>22</td>
</tr>
<tr>
<td>Private Credentials</td>
<td>144, 158</td>
</tr>
<tr>
<td>private information contracts</td>
<td>18</td>
</tr>
<tr>
<td>profiles</td>
<td>118</td>
</tr>
<tr>
<td>Protected Health Information (PHI)</td>
<td>30</td>
</tr>
<tr>
<td>Pseudonym</td>
<td>142</td>
</tr>
<tr>
<td>pseudonym system</td>
<td>143</td>
</tr>
<tr>
<td>pseudonym technology</td>
<td>141</td>
</tr>
<tr>
<td>pseudonym technology, accountability</td>
<td>142</td>
</tr>
<tr>
<td>pseudonym technology, anonymity</td>
<td>142</td>
</tr>
<tr>
<td>pseudonym-credentials</td>
<td>142</td>
</tr>
<tr>
<td>pseudonymity</td>
<td>146, 203, 227</td>
</tr>
<tr>
<td>pseudonymous identifiers</td>
<td>227</td>
</tr>
<tr>
<td>public key infrastructure system (PKI)</td>
<td>158</td>
</tr>
<tr>
<td>receiver</td>
<td>2</td>
</tr>
<tr>
<td>reputation</td>
<td>7</td>
</tr>
<tr>
<td>reputation network</td>
<td>8</td>
</tr>
<tr>
<td>reputation system</td>
<td>8</td>
</tr>
<tr>
<td>resource</td>
<td>211</td>
</tr>
<tr>
<td>right of privacy</td>
<td>2</td>
</tr>
<tr>
<td>risk identification</td>
<td>6</td>
</tr>
<tr>
<td>risk management</td>
<td>2</td>
</tr>
<tr>
<td>risks</td>
<td>2</td>
</tr>
<tr>
<td>role</td>
<td>204</td>
</tr>
<tr>
<td>role-based access control (RBAC)</td>
<td>180</td>
</tr>
<tr>
<td>safeguards</td>
<td>116</td>
</tr>
<tr>
<td>schemas</td>
<td>208</td>
</tr>
<tr>
<td>secure socket layer (SSL)</td>
<td>77</td>
</tr>
<tr>
<td>security</td>
<td>116</td>
</tr>
<tr>
<td>Security Assertion Markup Language (SAML)</td>
<td>204</td>
</tr>
<tr>
<td>security layers</td>
<td>129</td>
</tr>
<tr>
<td>sender</td>
<td>2</td>
</tr>
<tr>
<td>service-oriented architecture (SOA)</td>
<td>204</td>
</tr>
<tr>
<td>signature, digital</td>
<td>209</td>
</tr>
<tr>
<td>single sign-on</td>
<td>268</td>
</tr>
<tr>
<td>smart cards</td>
<td>79</td>
</tr>
<tr>
<td>SOAP</td>
<td>29, 229, 235</td>
</tr>
<tr>
<td>social engineering</td>
<td>81</td>
</tr>
<tr>
<td>spyware</td>
<td>116</td>
</tr>
<tr>
<td>subject</td>
<td>211</td>
</tr>
<tr>
<td>subject role</td>
<td>204</td>
</tr>
<tr>
<td>target</td>
<td>211</td>
</tr>
<tr>
<td>technology</td>
<td>120</td>
</tr>
<tr>
<td>telemedicine</td>
<td>61</td>
</tr>
<tr>
<td>third party (TTP)</td>
<td>181</td>
</tr>
<tr>
<td>threat risk analysis (TRA)</td>
<td>15</td>
</tr>
<tr>
<td>threats, environmental</td>
<td>124</td>
</tr>
<tr>
<td>threats, human</td>
<td>124</td>
</tr>
<tr>
<td>threats, natural</td>
<td>124</td>
</tr>
<tr>
<td>transaction logs</td>
<td>257</td>
</tr>
<tr>
<td>Trojan horses</td>
<td>116</td>
</tr>
<tr>
<td>trust mark</td>
<td>8</td>
</tr>
<tr>
<td>TRUSTe</td>
<td>8, 194</td>
</tr>
<tr>
<td>UDDI Business Registry</td>
<td>50</td>
</tr>
<tr>
<td>unforgeability</td>
<td>147</td>
</tr>
<tr>
<td>uninterruptible power supplies (UPS)</td>
<td>125</td>
</tr>
<tr>
<td>Universal Description, Discovery and</td>
<td></td>
</tr>
<tr>
<td>Integration (UDDI)</td>
<td>29</td>
</tr>
</tbody>
</table>

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.
unlinkability 147
user satisfaction 268
utility elicitation 4

V

valuation 2
Virtual private networks (VPNs) 77
virus 116
vulnerability scanning 133

W

W3C (see World Wide Web Consortium)
Web bugs 16
Web privacy enforcement engine (WPEE) 187
Web privacy policy (WPP) 189
Web services 204, 235
Web services architecture (WSA) 29
Web services architecture requirements 29
Web Services Description Language (WSDL) 29, 235
Web Services Discovery Agencies 42
wireless LAN (WLAN) 87
World Wide Web Consortium (W3C) 29

X

XACML (see also eXtensible Access Control Markup Language) 177, 204, 213
XACML context handler 222
XACML policies 231
XML (see also eXtensible Markup Language) 206, 229, 235
XML-based security standards 204
XML cryptography 209
XSLT (see also eXtensible Stylesheet Language Transformation) 185