Index

A

access control paradigm 204
Advanced Encryption Standard (AES) 2, 25
anonymous probing agents 189
Application Service Providers (ASPs) 273, 274
arithmetic primitives 36
ASIC 2
attribute certificate 66, 79
attribute ontology 184
Authority Information Access (AIA) 73
authorization certificate 66

B

basic constraints 76
biometry 138
block cipher algorithms 15
block ciphers 13
bridge CA 94

C

cando and do rules 160
Certificate Revocation List (CRL) 69
confidentiality 12
copyright protection 235
cryptography 1
cryptography on smart cards 107
CTCPEC 102

D

data authorization 295
Data Encryption Standard (DES) 21
data filters 194
dercando rules 160
Digital Government (DG) 182
Digital Home Networks (DHN) 99
digital rights 230
Digital Rights Management (DRM) 231, 259
Distributed Application Hosting Services (DAHSs) 273

E

e-business 274
Electronic Code Book (ECB) 19
Elliptic Curve Cryptosystems (ECC) 2, 33
eXtensible Access Control Markup Language (XACML) 246

eXtensible Markup Language (XML) 206, 279
eXtensible Rights Markup Language (XrML) 265

F

fields 6
finite fields 10
Flexible Authorization Framework (FAF) 149
FPGA 2

G

Global Provision and Obligation Set (GPOS) 170
Global System for Mobile Communication (GSM) 99

I

identity certificate 66
Integrated Circuit (IC) 99
integrity 12
Internet Protocol Security (IPSec) 327
ITSEC 101

J

Java™ Authentication and Authorization Service (JAAS) 326
Java™ Card API 119

L

Local ECM (LECM) 132

M

materialization 154
memories 105
Merkle Hash paths 224
Merkle signature 221
mesh 90
Microsoft .NET 317
Microsoft's Common Object Model (COM) 319
mobile privacy preserving agents 194
modular multiplication 39
Montgomery modular multiplication 42
MPEG-7 242
multimedia information 231
multimedia security 230

N

name constraints 76

O

Online Certificate Status Protocol (OCSP) 71
open platform card 119

P

policy constraints 76
privacy preservation requirement 181
Private Information Retrieval (PIR) 307
Private Personal Network (PPN) 134
profile-based paradigm 204
Public Key Infrastructure (PKI) 64
public-key algorithms 14
public-key certificate (PKC) 65

R

Random Number Generators (RNG) 106
reputation management model 186
Rights Management (RM) 259

S

scalability 218
Scalable Vector Graphics (SVG) 237, 250
SDSI/SPKI certificates 82
secure and selective dissemination of information 199
Secure Socket Layer (SSL) 283
security policies 294
Selective Dissemination of Information (SDI) 199
Semantic Web 177
service wrappers 191
SIM (Subscriber Identity Module) 99

Simple Object Access Protocol (SOAP) 320
smart card 99
SMIL 241
SSXDI system 208
steganography 233
stream ciphers 13
subscription-based paradigm 204
Sun ONE (J2EE) 317
symmetric-key algorithms 13
Systems on Programmable Chip (SoPC) 3
Systems-on-Chip (RSoC) 3

T

trust list 90
Trust Service Provider (TSP) 194

U

universal description, discovery and integration (279

V

VoiceXML 241

W

watermarking 234
Web privacy 179
Web Service Description Language (WSDL) 279

X

X509 66
XML 236