

Index

- 2G GBA 47, 175
- 3GPP 3, 30
- 3GPP2 3, 54

- A5/1 12
- A5/2 12, 175
- A5/3 12
- access control 161
 - for applications 110, 161
 - coarse-grained 161
 - fine-grained 161
 - policy setting 161
 - in Series 60 platform 162
 - using GUSS 79
- access independence 24
- ACL 164
- AKA 8, 13
 - 5-tuple 10
 - Authentication Vector 10
 - AUTN 10
 - CK 10
 - IK 10
 - permanent key for a subscriber 8
 - protocol 13
 - RAND 10
 - RES 10
 - SQN 8, 14
 - transports for signaling 14
 - XRES 10
- authentication proxy 72, 112
- Apache web server 156
- application separation 24
- application server 93, 106, 112, 133, 144, 153, 178
- attacks
 - active 12
 - BSF impersonation 176
 - downplay 177
 - fake base station 10
 - man-in-the-middle 14, 93, 176
 - masquerading 18
 - replay 11
 - SIM cloning 176
 - UE impersonation 175
- AuC 8, 55
- Authentication
 - proxy mode 106
 - referrer mode 106
- Bandit project 167
- Bluetooth 89, 154
- Broadcast mobile television 4, 122
- BSF 25, 30

- BSF address 34
- BSF Client, *see* GBA module
- BSF Proxy 180

- CA 17
- CableLabs 135
- calling line identifier 16
- CardSpace 107, 166
- CAVE 55
- CDMA 42, 54
- CDMA 1× 55
- CDMA 1× EV-DO 56
- CDMA2000 1× EV-DO 56
- certificate 16, 72, 106
- charging 177

- Diffie-Hellman key exchange 54
- digital signature 16
- DTN 140
- DVB-H 122

- EAP 14, 20
- EAP-AKA 14, 20
- EAP-SIM 20
- Early IMS security 15
- EPS 187
- E-UTRAN 187

- freshness 91, 141, 173, 184
- full IMS security 20

- GAA 1, 3, 23
 - authentication 39, 84
 - bootstrapping 26, 32, 34
 - deployability 153, 170, 189
 - generality 23
 - portability 189
- GAA-aware UIM 54, 56
- GBA 3, 23, 34, 41
- GBA module 31, 48, 86, 89, 160
- GBA Push 183
- GBA_H 135
- GBA_ME 33, 42
- GBA_U 42
- GEA1 12
- GEA2 12
- GEA3 12
- GPRS 11
- GSID 53, 80, 81, 82, 83, 156
- GSM 3
- GSM authentication
 - Kc 11
 - RAND 11
 - SRES 11
- GUSS 30, 79, 83, 156, 170, 177

- Higgins project 167
- HLR 8, 25, 30, 47, 96, 170
- home network 8
 - control of GAA applications 21, 24, 79
- home server 25, 32
- HSS 8, 25, 30, 32, 47, 54, 80, 83, 97, 125, 144, 170, 173
- HTML form based authentication 18, 154
- HTTP Digest 132, 136, 156, 157, 166, 176
- HTTP Digest AKA 8, 14, 44, 92
- HTTPS 109, 132, 135, 154

- IdP 107, 116, 166
- IKE 136
- IMPI 34, 42, 81, 82, 126, 132, 178
- IMS 15, 20, 41, 134, 144, 171
 - I-CSCF 144
 - S-CSCF 144
- IMSI 8, 12, 24, 34, 82, 84, 157, 178
- IMSI_S 58
- IMSI_S2 58
- integrating GAA
 - with Apache web server 156
 - with application servers 153
 - with Identity Management Systems 165
 - with J2EE servers 157
 - into large networks 178
 - with Liberty ID-FF 167
 - into mobile networks 170
 - with OS Security 159
- Interfaces Ut 133
- interoperator GAA 89

- IP address binding 16
- IPsec 20
- ISIM 15, 41, 98

- KASUMI 11
- KDF 29, 34, 38, 42, 48, 94
- Kerberos 19
- key agreement 2
- key confidentiality 11, 91, 109, 132, 140
- key derivation 29, 38, 42, 93
- key distribution service 72, 74, 99
 - terminal to remote device 74
 - terminal to terminal 142
 - UICC to terminal 77
- key lifetime 12, 24, 173
- Ks_co 137
- Ks_ext_NAF 42
- Ks_int_NAF 42

- LDAP 154
- legacy UIM 54
- Liberty Alliance 99, 106, 116, 166
- LTE 187
- LTKM 126

- MAC 10
- MAP 55, 97
- MBMS 4, 99, 122
- MCC 34, 178
- ME 10, 34
- MGV-S/F 126, 130
- MIP 187
- MNC 34, 178
- Mobile IP 56
- mobile TV *See* broadcast mobile TV
- MPEG-2 125
- MSIN 178
- MSISDN 24, 137
- mutual authentication 91

- NAF 25, 30
 - Key Center 4, 74, 142
 - library 153, 155, 158
- NASS-IMS bundled authentication 16

- Oakley group 54
- OMA SUPL 132
- OMA XDM 132
- onetime password 136
- OpenID 107, 116, 166
- OS Security 159

- passwords 18
- PEK 125
- PIN 3
- PKI 16
- PKI portal 72
- PLMN 178
- privacy 84, 185
- protection of original infrastructure 24
- proxy mode 106, 112
- PSK TLS 33, 96, 106, 111

- RA 17
- radio layer security 14
- RADIUS 154
- referrer mode 106, 116
- replay attacks 11
- RNC 11
- RP 107, 166
- R-UIM 41

- SAML 166
- SAP 89
- SCTP 97
- SecureID 136
- security objectives 91
- SEK 125
- separation of keys 16
- Series 60
 - access control 162
 - GAA Server 162
- SGSN 10
- SIM 11, 41, 98
- SMS 19, 139, 170
- SP 107, 166
- split terminal 87, 154
- SSC 72
- SSO 99, 119
- STKM 125

- STS 107
- subscriber certificate 72, 99, 106
- Symbian OS 162
 - capabilities 162
 - platform security 162
 - SID 163
 - trusted applications 162
 - untrusted applications 162
 - VID 164
- TCAP 97
- TISPAN 15, 133
- TLS 17
- TMSI 12, 84, 187
- traitor tracing 130
- Ua interface 27, 32, 39
- Ub interface 26, 31, 32, 34
- UE 12, 26
- UICC 10, 26
- UMTS 3, 8
 - access security 9
- UMTS AKA *See* AKA
- UMTS Authentication Vector 10
- UMTS security 8
- usability 84, 86
- username/password 84, 105, 154
- USIM 10, 98
- USS 53, 79, 83, 112, 155, 170, 177
 - for BSF 80
 - for NAF 81
- UTRAN 187
- VLR 10
- VPN 136
- WAP gateway 106
- WPKI 18
- WSDL 153
- WS-SX 116, 166
- XCAP 132
- Zh interface 26, 32
- Zh' interface 32, 48, 171
- Zn interface 28, 32, 90
- Zn' interface 28, 90
- Zn proxy 28, 90