

---

# Index

## A

abstraction, 144. *See also* TCS

access

data to specific PCs, locking, 198-199

DMA, 246

FAT, 185

group hard disks, 194-196

localities, 75

administration

devices, 231-240

DRM, 200

functions, 279-288

PKCS#11, 161

TCS, 146-152

TSS, 94

VPN endpoints, 208-210

administrators, TPM commands, 293

adware, 7

AES (Advanced Encryption Standard),

19, 182

algorithms

hash, 88-89

SHA-1, 15

SHA1, 97-99

symmetric, 181-193

AMD Secure Virtual Machine, 72-74

analysis, security, 26-28

APIs (application programming interfaces), 3

PKCS#11, 157-163

TSS functionality, 77

applications

clients, 9

encryption, 182

helper programs, 193

migration, 169-178

PKCS#11, 157-169

TCS, 144-145

TSS, 77

utility functions, 104, 107

validation data structure, 101-102

**architecture**

- backup/maintenance, 231-235
- Storage Root Key, 34
- TSS, 77-79

**assignment of key certificates, 235-237****asymmetric keys, 19-22****Atmel 1.1b TPM, 47****attacks**

- BORE, 260
- changing threats of, 4-8
- cost of, 3-4
- hammering, 41
- shoulder surfing, 244
- types of, 26

**attestation, 144****Attestation Identity Key, 111****auditing functions, 273-274****authentication**

- biometrics, 218-220
- COTS, 225
- credit cards, 211-213
- DAA, 260-269
- HIPAA compliance, 222-225
- HMAC, 185, 243
- hoteling, 214-216
- IP telephony, 226
- IPSec, 226-227
- multiple users, 213-214
- network switches, 228-230
- PKI, 216-218
- service meters, 227-228
- smart cards, 220-221
- trusted endpoints, 221-222
- virtual dongles, 221

**authorities**

- DAA, 260-269
- delegation of, 210-211

**authorization, 20-22**

- delegation, 253-259
- locality, 269

**OSAP, 20**

- policy objects, 82-85
- TPM objects, 81-82
- trusted display, 246-247
- trusted path, 243-246

**avoiding exposure, 41****B****backup, 196-198, 231-235****basic key structure, 31****behavior of PCRs, 269-270****binding**

- data, 127-132
- keys, 36
- section, 151

**biometrics, 218-220****BIOS**

- boot sequences, 14-18
- TPM, 59-62

**blob migration, 232****blocks, CBC, 184****booting**

- loaders, 16
- sequences, 14-18
- trusted boot, 69-76

**bootstrap loaders, 60****BORE (Break Once Run Everywhere)**

- attacks, 260

**broadband eavesdropping, 8****buffer overflow, 5****C****C, TSS functions, 323-331****CA (Certificate Authority), 194****callback functions, 99-100****cards**

- NICs, 226-227
- smart. *See* smart cards

- categories of attacks, 4-8
- CBC (Cipher Block Chaining), 184
- certificates
  - DAA, 260-269
    - key assignment of, 235-237
- checking TPM configuration, 67
- Cipher Block Chaining (CBC), 184
- classification of keys, 35-36
- clearing TPM, 63
- client applications, security, 9
- CMKs (Certified Migratable Keys), 92, 249-253
- codes
  - HMAC, 185
  - TCS, 145
  - TSS return, 93-94
- commands
  - MigrateMigrationBlob, 232
  - Tcsi\_EnumRegisteredKeys, 285
  - TPM, 63-66, 78, 293-301
    - TPM\_CreateWrapKey, 66
    - TPM\_EvictKey, 66
    - TPM\_GetCapability, 64
    - TPM\_LoadKey, 66
    - TPM\_PcrRead, 65
    - TPM\_ReadPubek, 65
    - TPM\_Reset, 64
    - TPM\_Seal, 67
    - TPM\_Sign, 67
    - TPM\_TakeOwnership, 66-67
    - TPM\_Unseal, 67
  - TPM\_ChangeAuthOwner, 39
  - Tcsi\_Admin\_TSS\_MaxTimePerLocality, 282
  - Tcsi\_Admin\_TSS\_SessionPerLocality, 281
  - Tspi\_Context\_CloseSignTransport, 278
  - Tspi\_Context\_GetRegisteredKeyByPublicInfo, 286-287
  - Tspi\_Context\_GetRegisteredKeyByUUID, 287
  - Tspi\_Context\_GetRegisteredKeyByUUID2, 287-288
  - Tspi\_Context\_RegisterKey, 283
  - Tspi\_Context\_SetTransEncryptionKey, 278
  - Tspi\_Context\_UnregisterKey, 284
  - Tspi\_DecodeBER\_TssBlob, 289
  - Tspi\_EncodeDER\_TssBlob, 288-289
  - Tspi\_GetRegisteredKeyByUUID, 285-286
  - Tspi\_Key\_CMKConvertMigration, 252-253
  - Tspi\_Key\_CMKCreateBlob, 250-251
  - Tspi\_Key\_MigrateKey, 251
  - Tspi\_NV\_DefineSpace, 271
  - Tspi\_NV\_ReadValue, 272
  - Tspi\_NV\_ReleaseSpace, 271-272
  - Tspi\_NV\_WriteValue, 272
  - Tspi\_TPM\_CheckMaintenancePolicy, 282
  - Tspi\_TPM\_CMKApproveMA, 252
  - Tspi\_TPM\_CMKSetRestrictions, 250
  - Tspi\_TPM\_CreateMaintenanceArchive, 236
  - Tspi\_TPM\_CreateRevocableEndorsementKey, 279-280
  - Tspi\_TPM\_CreateTicket, 252
  - Tspi\_TPM\_DAA\_ARDecrypt, 268-269
  - Tspi\_TPM\_DAA\_IssueInit, 266
  - Tspi\_TPM\_DAA\_IssuerKeyVerification, 265
  - Tspi\_TPM\_DAA\_IssueSetup, 265-266
  - Tspi\_TPM\_DAA\_JoinCreateDaaPubKey, 263
  - Tspi\_TPM\_DAA\_JoinInit, 262-263
  - Tspi\_TPM\_DAA\_JoinStoreCredential, 264
  - Tspi\_TPM\_DAA\_RevokeSetup, 268
  - Tspi\_TPM\_DAA\_Sign, 264

- Tspi\_TPM\_DAA\_VerifyInit, 267
  - Tspi\_TPM\_DAA\_VerifySignature, 267
  - Tspi\_TPM\_Delegate\_AddFamily, 255
  - Tspi\_TPM\_Delegate\_CacheOwner-Delegation, 257
  - Tspi\_TPM\_Delegate\_CreateDelegation, 257
  - Tspi\_TPM\_Delegate\_GetFamily, 256
  - Tspi\_TPM\_Delegate\_InvalidateFamily, 256
  - Tspi\_TPM\_Delegate\_ReadTables, 259-260
  - Tspi\_TPM\_Delegate\_UpdateVerification-Count, 258
  - Tspi\_TPM\_Delegate\_VerifyDelegation, 259
  - Tspi\_TPM\_GetAuditDigest, 274
  - Tspi\_TPM\_KeyControlOwner, 284-285
  - Tspi\_TPM\_KillMaintenanceFeature, 237
  - Tspi\_TPM\_ReadCurrentCounter, 275
  - Tspi\_TPM\_ReadCurrentTicks, 276
  - Tspi\_TPM\_RevokeEndorsementKey, 280-281
  - Tspi\_TPM\_SetOrdinalAuditStatus, 273
  - Tspi\_TPM\_TickStampBlob, 276-277
  - TSS, 303-312
  - communication
    - through BIOS, 59-62
    - through TDDL, 62-66
    - TPM\_TakeOwnership command, 66-67
  - comparing keys, 34-35
  - compliance, HIPAA, 222-225
  - composite objects, PCE, 89-90
  - configuration
    - biometrics, 218-220
    - callback functions, 99-100
    - features not included, 25
    - identities, 23
    - internal random number generation, 24-25
    - keys, 34-35, 103-107
    - multiple user environments, 23-24
    - passwords, 83
    - PCRs. *See* PCRs
    - PKCS#11, 162-169
    - PKI, 216-218
    - smart cards, 220-221
    - signatures, 22-23
    - storage, 18-22
    - symmetric keys, 127-135
    - TPM, 67
    - trusted endpoints, 221-222
    - WSDL, 146-152
  - connection version, 81
  - content protection, 200-201
  - context objects, 80-81, 324, 331
  - convenience functions, 279-289
  - core services, 77, 141
  - cost of attacks, 3-4
  - Counter Object, 327, 331
  - counters
    - monotonic, 275
    - tick, 276-277
  - CreateSecureMigratableKeyBlob
    - function, 322
  - credit card endpoints, 211-213
  - cryptography, 157
    - administration, 161
    - design, 162
    - migration, 169-178
    - openCryptoki design, 162-169
    - overview of, 158
    - RSA key restrictions, 159-160
    - tokens, 158-159
  - cybercrime, cost of, 3-4
- D**
- DAA (Direct Anonymous Authentication), 92, 260-269
  - daisy chains, 33
  - data binding, 127-132
  - Data Integrity Register (DIR), 91

- data objects, 87, 91-92
  - data sealing, 132-135
  - DecryptFile function, 321
  - DecryptFileLoad function, 322
  - decryption, 193
  - delegation, 253-254
    - of authority, 210-211
    - commands, 255-260
    - family objects, 92
    - without allowing migration, 211
  - Delegation Table object, 328, 331
  - design. *See also* configuration
    - platforms, 14-18
    - TPM, 9-10
  - TSS
    - configuring callback functions, 99-100
    - memory management, 94
    - overview of, 77-79
    - persistent key storage, 95-97
    - portable data, 94-95
    - return codes, 93-94
    - signing/verifying data, 97-99
    - TSP, 79-92
    - Tspi, 79
    - validation data structure, 101-102
  - devices
    - administration, 231
      - assignment of key certificates, 235-237
      - backup/maintenance, 231-235
      - key recovery, 239-240
      - time reporting, 237-238
      - tools, 240
    - drivers, 59-66, 332. *See also* drivers
    - TDDL, 45-46, 77
      - TCG 1.1b specification, 47-50
      - TPM 1.2 specification, 50-58
    - virtual dongles, 221
  - Digital Rights Management (DRM), 200
  - digital signature security, 40-41
  - DIR (Data Integrity Register), 91
  - Direct Anonymous Authentication. *See* DAA
  - direct memory access (DMA), 246
  - disks, hard, 191-196
  - DMA (direct memory access), 246
  - dongles, virtual, 221
  - drivers
    - commands, 332
    - TDDL, 45-46, 77
      - TCG 1.1b specification, 47-50
      - TPM 1.2 specification, 50-58
    - TPM
      - communication through BIOS, 59-62
      - communication through TDDL, 62-66
  - DRM (Digital Rights Management), 200
  - dynamic root of trust measurements, 71-72
- ## E
- EK (endorsement key), 29
  - electrical usage service meters, 227-228
  - electronic eavesdropping, 8
  - element types, 148
  - email
    - phishing, 7
    - secure time reporting, 237-238
    - sniffing, 8
  - enabling TPM, 63
  - EncryptFile function, 321
  - encryption
    - AES, 19, 182
    - CBC, 184
    - data binding, 127-129, 132
    - data objects, 87
    - files, 136-138
      - backup facilities, 196-198
      - for group access/hard disks, 194-196
      - sending, 183-191
      - for storage on hard disks, 191-193
    - I/O, 193
    - OAEP, 128, 183, 239-240
    - software, 182

endorsement key (EK), 29, 216-218

Endorsement objects, 330

endpoints

credit cards, 211-213

trusted, 221-222

VPNs, 208-210

environments

multiple users, 23-24

platforms, 14-18

errors, parsing, 5

Ethernets, 228-230

exposure, avoiding, 41

## F

FAT (file access table), 185

fax security, 202

features not included, 25

file access table (FAT), 185

files

data specific to, locking, 198-199

encryption. *See* encryption

WSDL, 145, 147-149

finite resources, 142-143

flags, 237

flash storage, 91

formatting

keys, 103-107

passwords, 83

symmetric keys, 127-138

WSDL, 146-152

free seating, 213. *See also* hoteling

functionality

APIs, 77

PCRs, 269-270

functions

administration, 279

Tcsi\_EnumRegisteredKeys command,  
285

Tcsi\_Admin\_TSS\_MaxTimePer-  
Locality command, 282

Tcsi\_Admin\_TSS\_SessionPerLocality  
command, 281

Tspi\_Context\_GetRegisteredKeyBy-  
PublicInfo command, 286-287

Tspi\_Context\_GetRegisteredKeyBy-  
UUID command, 287

Tspi\_Context\_GetRegisteredKeyBy-  
UUID2 command, 287-288

Tspi\_Context\_RegisterKey  
command, 283

Tspi\_Context\_UnregisterKey  
command, 284

Tspi\_DecodeBER\_TssBlob  
command, 289

Tspi\_EncodeDER\_TssBlob command,  
288-289

Tspi\_GetRegisteredKeyByUUID  
command, 285-286

Tspi\_TPM\_CheckMaintenancePolicy  
command, 282

Tspi\_TPM\_CreateRevocable-  
EndorsementKey command, 279-280

Tspi\_TPM\_KeyControlOwner  
command, 284-285

Tspi\_TPM\_RevokeEndorsementKey  
command, 280-281

auditing, 273

Tspi\_TPM\_GetAuditDigest command,  
274

Tspi\_TPM\_SetOrdinalAuditStatus  
command, 273

callback, 99-100

CreateSecureMigratableKeyBlob, 322

DecryptFile, 321

DecryptFileLoad, 322

EncryptFile, 321

files, 136-138

grouping, 154-155

keys, 35-36

libraries, 321-322

LoadSecureMigratableKeyBlob, 322  
 MyFunc\_CreateAIK(), 111  
 MyFunc\_CreateKeyHierarchy(), 116  
 MyFunc\_CreatePubKey(), 104  
 MyFunc\_CreateTPMKey(), 107  
 MyFunc\_GetRandom(), 116  
 MyFunc\_WrapKey(), 108  
 prototypes, 150-151  
 Tcsi\_GetCapability(), 149  
 Tcsi\_OpenContext(), 149  
 TSS, 323-331  
 TSS\_buildbuff(), 65  
 utility, 104, 107

## G-H

generating

CMKs, 249-253  
 internal RNG, 24-25  
 migratable keys, 34-35  
 random numbers, 183

groups

DAA, 260-269  
 delegation, 253-260  
 functions, 154-155

grub, 59

gSOAP tool, 152-154

hackers, 4-8

hammering, 19, 41

handoff procedures, 39

hard disks, 191-196

hardware, 243-247

hashed message authentication code (HMAC),  
 185, 243

hashes, 84, 88-89

headers, 147

helper programs, 193

hierarchies, keys, 103

HIPAA (Health Insurance Portability and  
 Accountability Act), 181, 222-225  
 HMAC (hashed message authentication code),  
 185, 243  
 hoteling, 213-216, 219

## I

I/O encryption/decryption keys, 193

IBM libtpm package, 62

identification (secure)

biometrics, 218-220

COTS, 225

credit card endpoints, 211-213

delegation, 210-211

HIPAA compliance, 222-225

hoteling, 214-216

IP telephony, 226

IPSec, 226-227

login password storage, 208

multiple users, 213

network switches, 228-230

PKI, 216-218

service meters, 227-228

smart cards, 220-221

trusted endpoints, 221-222

virtual dongles, 221

VPN endpoints, 208-210

identities, 23, 36

Identity Key objects, 330

indexes, 89-90

infrastructure, PKI, 207

integrity, platforms, 37-40

interfaces

APIs, 3, 77

NICs, 226-227

PKCS#11, 157

administration, 161

design, 162

migration, 169-178

- openCryptoki design, 162-169
  - overview of, 158
  - RSA key restrictions, 159-160
  - tokens, 158-159
- TCS, 145
- TDDL, 45-46
  - TCG 1.1b specification, 47-50
  - TPM 1.2 specification, 50-58
- Tspi, 79
- internal random number generator (RNG), 24-25
- Internet security, printing, 202
- intranet security, printing, 201
- IPSec, 226-227
- IP telephony, 226
- isolation of users, 23-24

## J–K

- kernels, 15
- keyboards, 244-246
- keys
  - architecture, 232
  - asymmetric, 19-22
  - Attestation Identity Key, 111
  - basic structure, 31
  - certificates, 235-237
  - CMKs, 92, 249-253
  - content protection, 200-201
  - context objects, 80-81
  - delegation, 210-211, 253-259
  - EK, 29
  - endorsement, 216-218
  - group hard disk storage, 194-196
  - hierarchies, 103
  - I/O encryption/decryption, 193
  - identities, 23
  - IPSec, 226-227
  - leaf, 32
  - migration, 34-35, 231
  - multiple user environments, 23-24

- objects, 85-87, 324, 329
  - PKCS#11, 157-169
  - PKI, 207
  - Public, 183-191
  - recovery, 239-240
  - Rijndael, 190
  - RSA, 158-160
  - secure migration storage, 203-205
  - signatures, 22-23, 40-41
  - signing/verifying data, 97-99
  - SRK, 29-31, 33
  - storage, 95-97
  - symmetric, 19, 127-138
  - TCS, 143
  - types of, 35-36
  - utility functions, 104, 107
- known public keys, sending files with, 190-191

## L–M

- Lagrande Technology (LT), 72
- leaf keys, 32
- libraries
  - functions, 321-322
  - TDDL, 45-55, 77
  - TSP, 80-81
- libtpm package (IBM), 62
- linking to symmetric algorithms, 181-193
- loading keys, 143
- LoadSecureMigratableKeyBlob function, 322
- local requests, 141
- local service provider, TCS, 144-145
- locality, 75-76, 269
- locking data to specific PCs, 198-199
- login, password storage, 208
- LT (Lagrande Technology), 72
- MA (Migration Authority), 249
- maintenance, 231-235
  - platform integrity, 39-40
  - SRK, 29-33



malicious programs. *See* adware; spyware; viruses

management. *See* administration

mask generation function 1(MGF1), 183

MaskedSymmetricKey, 186

measurements

- dynamic root of trust, 71-72
- platforms, 14-18

memory

- DMA, 246
- management, 94

messages

- HMAC, 185
- secure time reporting, 237-238
- TCS, 150

meters, secure identification for, 227-228

MGF1 (mask generation function 1), 183

MigrateMigrationBlob command, 232

migration

- authorization data, 239
- blobs, 232
- CMKs, 249-253
- delegation, 210-211
- keys, 34-35, 231
- PKCS#11, 169-178
- SRK, 33
- storage security, 203-205

Migration Authority (MA), 249

Migration Selection Authority (MSA), 249

migrationBlob, 204

military security solutions, COTS, 225

misconfigured programs, 7

models, usage, 21

modes, secret, 82-84

monotonic counters, 275

Monte Carlo routine, 25

MSA (Migration Selection Authority), 249

multiple signatures, privacy and, 41

multiple users

- environments, isolation of users, 23-24
- on single systems, 213

MyFunc\_CreateAIK() function, 111

MyFunc\_CreateKeyHierarchy(), 116

MyFunc\_CreatePubKey() function, 104

MyFunc\_CreateTPMKey() function, 107

MyFunc\_GetRandom() function, 116

MyFunc\_WrapKey() function, 108

## N

National Security Agency (NSA), 182

natural gas usage service meters, 227-228

networks

- switches, 228-230
- VPNs, 208-210, 226-227

NICs (network interface cards), 226-227

non-migratable keys, 34-35

non-volatile data objects, 91

nonce, 17

numbers

- generating, 183
- internal RNG, 24-25

NVRAM, 270

- commands, 271-272
- non-volatile data objects, 91
- objects, 327, 330

## O

OAEP (Optimal Asymmetric Encryption Padding), 128, 183, 239-240

Object Identifier (OID), 97

Object Independent Authorization Protocol (OIAP), 66

Object Specific Authorization Protocol (OSAP), 20, 66

objects

- storage, 18-20
- TSP, 79
- context, 80-81
- DAA, 92
- delegation family, 92

- encrypted data, 87
  - hash, 88-89
  - keys, 85-87
  - migratable data, 92
  - non-volatile data, 91
  - PCR composite, 89-90
  - policy, 82-85
  - TPM, 81-82
  - Tspi, 79
  - TSS functions, 323-331
  - types of, 79-89, 92
  - offloading keys, TCS, 143
  - OIAP (Object Independent Authorization Protocol), 66
  - OID (Object Identifier), 97
  - openCryptoki, 162-169
  - optimal asymmetric encryption padding. *See* OAEP
  - OSAP (Object Specific Authorization Protocol), 20, 66
  - out parameters, 149-150
  - ownership, 66-67
- P**
- Pacifica, 72
  - packages, IBM libtpm, 62
  - padding OAEP, 128, 183
  - parsing errors, 5
  - passphrases, 183, 193
  - passwords, 83, 208
  - PCRs (Platform Configuration Registers), 10, 37-39
    - behavior, 269-270
    - boot sequences, 15
    - composite objects, 89-90
    - objects, 325, 330
    - passphrases, 193
    - standard meaning of, 60
    - TCS, 143
    - TPM commands, 295
    - trusted boot with static root of trust, 69-71
    - trusted display, 247
  - PCs (personal computers), 13
    - data specific to, locking, 198-199
    - hoteling, 214-216
    - sharing, 213
    - virtual dongles, 221
  - persistent key storage, TSS, 95-97
  - personal computers. *See* PCs
  - pharming, 7
  - phishing, 7
  - PKCS#11 (Public Key Cryptography Standard number 11), 157
    - administration, 161
    - design, 162
    - migration, 169-178
    - openCryptoki design, 162-169
    - overview of, 158
    - RSA key restrictions, 159-160
    - tokens, 158-159
  - PKI (Public Key Infrastructure), 207, 216-218, 236
  - Platform Configuration Registers. *See* PCRs
  - platforms
    - integrity, 37-40
    - reporting, 14-18
    - TSS, 94-95
  - Policy objects, 81-85
  - portable data, TSS, 94-95
  - portable security tokens, 15
  - ports, virtual dongles, 221
  - power management, 295
  - printing, 201-202
  - privacy
    - biometrics, 219
    - signatures, 41
    - TCS, 154-155
  - PRNGs (pseudo random number generators), 24
  - proof of locality, 75-76

## protocols

- IP, 226
  - IPSec, 226-227
  - OIAP, 66
  - OSAP, 20, 66
  - SET, 212
  - SOAP, 277
  - Verified by VISA, 212
- prototypes, 150-151
- Pubek (public endorsement key), 65
- Public Key Cryptography Standard number 11. *See* PKCS#11
- Public Key Infrastructure. *See* PKI
- public keys
- control of, 35
  - files, 183-191

**Q-R**

- queries, nonce, 17
- quote operations, 89-90
- random numbers, generating, 24-25, 183
- recording boot sequences, 14-18
- recovery, 234, 239-240
- references, TSS commands, 303-313
- registers, 91. *See also* PCRs
- remote identification, 221-222
- Remote Procedure Calls. *See* RPCs
- remote requests, 141
- reports
- platforms, 14-18
  - time, 237-238
- requests, TCS, 146-155
- resources, managing, 142-143
- restrictions, RSA keys, 159-160
- return codes, TSS, 93-94
- rights, DRM, 200
- Rijndael keys, 190
- RNG (random number generator), internal, 24-25
- RPCs (Remote Procedure calls), 146
- RSA keys, types of, 158-159

**S**

- Sarbanes-Oxley Act, 181
- scalability, 71
- Schell, Roger, 9
- sealing data, 89, 132-135
- secret mode, 82-84
- secrets, types of, 84
- sections, 151-154
- secure boot, 17
- Secure Electronic Transaction (SET) protocol, 212
- Secure Hash Algorithm 1 (SHA-1), 15
- secure identification
- biometrics, 218-220
  - COTS, 225
  - credit card endpoints, 211-213
  - delegation, 210-211
  - HIPAA compliance, 222-225
  - hoteling, 214-216
  - IP telephony, 226
  - IPSec, 226-227
  - login password storage, 208
  - multiple users, 213
  - network switches, 228-230
  - PKI, 216-218
  - service meters, 227-228
  - smart cards, 220-221
  - trusted endpoints, 221-222
  - virtual dongles, 221
  - VPN endpoints, 208-210
- Secure Virtual Machine, 72-74
- security
- analysis, 26, 28
  - applications, 9
  - backup/maintenance, 231-235
  - changing threats to, 4-8
  - content protection, 200-201
  - data to specific PCs, locking, 198-199
  - faxes, 202
  - hardware, 243-247
  - identities, 23

- keys, 235
- migration, 203-205
- printing, 201-202
- signatures, 22-23, 40-41
- SRK, 29-33
- storage, 18-22, 181-193
- TCS, 142
- time reporting, 237-238
- tokens, 15
- TPM, 9-10
- sending files, 183-191
- sequences, boot, 14-18
- servers, 208-210, 228-230
- service meters, secure identification, 227-228
- service providers
  - TCS, 144-145
  - TSP, 77-89, 90-92
  - Tspi, 79
- service section, 151-154
- services, 77, 141
- sessions, 277-278
- SET (Secure Electronic Transaction)
  - protocol, 212
- SHA-1 (Secure Hash Algorithm 1), 15, 88-89, 97-99
- Shamir, Adi, 41
- sharing PCs, 213
- shoulder surfing attack, 244
- signatures, 22-23, 36-41
- signing data, 97-99
- SKINIT instruction, 72, 75
- smart cards, 211-213, 220-221
- sniffing email, 8
- SOAP, 277
- social engineering, 7-8
- software. *See* applications
- special keyboards, 244-246
- spyware, 7
- SRK (Storage Root Key), 23, 29-33, 296-298

- stacks
  - secure migration storage, 203-205
  - TCS, 144
  - TSS, 77
- static root of trust, trusted boot with, 69-71
- status, platforms, 14-18
- storage
  - backup facilities, 196-198
  - content protection, 200-201
  - data to specific PCs, 198-199
  - delegation of authority, 210-211
  - design, 18-22
  - flash, 91
  - group hard disks, 194-196
  - keys, 36
    - data sealing, 132-135
    - TSS persistent, 95-97
  - login password, 208
  - migration, 203-205
  - security, 181-193
- Storage Root Key (SRK), 23, 29-33
- stubs, gSOAP, 154
- symmetric algorithms, 181-193
- symmetric keys, 19, 127-138

## T

- tables
  - delegation, 253-260
  - FAT, 185
- TCB (trusted computing base), 71
- TCG 1.1b specification, 47-50
- TCG core service (TCS), 77
- TCG device driver library (TDDL), 77
- TCG service provider interface. *See* Tspi
- TCG service provider. *See* TSP
- TCG\_HashLogExtendEvent, 60
- TCG\_PassThroughToTPM, 60
- TCG\_StatusCheck, 60

- TCS (TSS Core Service), 141
  - binding section, 151
  - function prototypes, 150-151
  - gSOAP tool, 152-154
  - implementing, 145-152
  - in/out parameters, 149-150
  - messages, 150
  - overview of, 141-145
  - privacy, 154-155
  - service section, 151-154
- Tcsi\_EnumRegisteredKeys command, 285
- Tcsi\_GetCapability( ) function, 149
- Tcsi\_OpenContext( ) function, 149
- TDDL (TCG device driver library), 45-46, 77
  - communication through, 62-66
  - TCG 1.1b specification, 47-50
  - TPM 1.2 specification, 50-58
- telephony, IP, 226
- Thompson, Michael, 9
- threats, 4-8
- tick counters, 276-277
- Tick Object, 327, 331
- tickets, 250
- time of measurement, 71
- time reporting, 237-238
- tokens, 15, 158-159
- tools
  - gSOAP, 152-154
  - TPM, 240
- TPM (Trusted Platform Module), 3
  - administration, 231-240
  - applying, 9-10
  - Atmel 1.1b, 47
  - BIOS, 59-62
  - clearing, 63
  - commands, 78, 293-301
  - configuring, 67
  - device drivers, 45-58
  - enabling, 63
  - functions, 321-322
  - hardware, 243-247
  - keys
    - creating hierarchies, 103
    - objects, 85-87
    - types of, 35-36
    - utility functions, 104, 107
  - objects, 81-82, 323-324, 328
  - platform integrity, 37-40
  - smart cards, 220-221
  - SRK, 32
  - symmetric keys, 127-138
  - TDDL, 63-67
  - TDL, 62
  - trusted endpoints, 221-222
- TPM 1.2 specification, 50-58
- TPM\_AuthorizeMigrationKey command, 194
- TPM\_ChangeAuthOwner command, 39
- TPM\_CreateMigrationBlob command, 194
- TPM\_CreateWrapKey command, 66, 194
- TPM\_EvictKey command, 66
- TPM\_GetCapability command, 64
- TPM\_LoadKey command, 66
- TPM\_PcrRead command, 65
- TPM\_Quote command, 199
- TPM\_ReadPubek command, 65
- TPM\_Reset command, 64
- TPM\_Seal command, 67, 199
- TPM\_Sign command, 67
- TPM\_TakeOwnership command, 66-67
- TPM\_Unseal command, 67
- tracking, 253-260
- transactions, 212. *See also* credit cards
- transport sessions, 277-278
- Trojan horses, 7, 41
- troubleshooting SRK, 29-33
- trusted boot, 17, 69-75
- trusted computing base (TCB), 71
- Trusted Computing Group Software Stack.
  - See* TSS
- trusted endpoints, 221-222

- trusted path, 243-247
- Trusted Platform Module. *See* TPM
- Tsci\_Admin\_TSS\_MaxTimePerLocality command, 282
- Tsci\_Admin\_TSS\_SessionPerLocality command, 281
- TSP (TCG service provider), 77, 79
  - context objects, 80-81
  - DAA objects, 92
  - delegation family objects, 92
  - encrypted data objects, 87
  - hash objects, 88-89
  - key objects, 85-87
  - migratable data objects, 92
  - non-volatile data objects, 91
  - PCR composite objects, 89-90
  - policy objects, 82-85
  - TPM objects, 81-82
- Tspi (TCG service provider interface), 79
- Tspi\_Context\_CloseSignTransport command, 278
- Tspi\_Context\_GetRegisteredKeyByPublicInfo command, 286-287
- Tspi\_Context\_GetRegisteredKeyByUUID command, 287
- Tspi\_Context\_GetRegisteredKeyByUUID2 command, 287-288
- Tspi\_Context\_RegisterKey command, 283
- Tspi\_Context\_SetTransEncryptionKey command, 278
- Tspi\_Context\_UnregisterKey command, 284
- Tspi\_Data\_Bind\_Bind command, 195
- Tspi\_Data\_Unbind command, 195
- Tspi\_DecodeBER\_TssBlob command, 289
- Tspi\_EncodeDER\_TssBlob command, 288-289
- Tspi\_GetRegisteredKeyByUUID command, 285-286
- Tspi\_Key\_CMKConvertMigration command, 252-253
- Tspi\_Key\_CMKCreateBlob command, 250-251
- Tspi\_Key\_MigrateKey command, 251
- Tspi\_Key\_TPM\_CMKApproveMA command, 252
- Tspi\_NV\_DefineSpace command, 271
- Tspi\_NV\_ReadValue command, 272
- Tspi\_NV\_ReleaseSpace command, 271-272
- Tspi\_NV\_WriteValue command, 272
- Tspi\_TPM\_CheckMaintenancePolicy command, 282
- Tspi\_TPM\_CMKSetRestrictions command, 250
- Tspi\_TPM\_CreateMaintenanceArchive command, 236
- Tspi\_TPM\_CreateRevocableEndorsementKey command, 279-280
- Tspi\_TPM\_CreateTicket command, 252
- Tspi\_TPM\_DAA\_ARDecrypt command, 268-269
- Tspi\_TPM\_DAA\_IssueInit command, 266
- Tspi\_TPM\_DAA\_IssuerKeyVerification command, 265
- Tspi\_TPM\_DAA\_IssueSetup command, 265-266
- Tspi\_TPM\_DAA\_JoinCreateDaaPubKey command, 263
- Tspi\_TPM\_DAA\_JoinInit command, 262-263
- Tspi\_TPM\_DAA\_JoinStoreCredential command, 264
- Tspi\_TPM\_DAA\_RevokeSetup command, 268
- Tspi\_TPM\_DAA\_Sign command, 264
- Tspi\_TPM\_DAA\_VerifyInit command, 267
- Tspi\_TPM\_DAA\_VerifySignature command, 267
- Tspi\_TPM\_Delegate\_AddFamily command, 255
- Tspi\_TPM\_Delegate\_CacheOwnerDelegation command, 257

Tspi\_TPM\_Delegate\_CreateDelegation  
command, 257

Tspi\_TPM\_Delegate\_GetFamily  
command, 256

Tspi\_TPM\_Delegate\_InvalidateFamily  
command, 256

Tspi\_TPM\_Delegate\_ReadTables command,  
259-260

Tspi\_TPM\_Delegate\_UpdateVerification-  
Count command, 258

Tspi\_TPM\_Delegate\_VerifyDelegation  
command, 259

Tspi\_TPM\_GetAuditDigest command, 274

Tspi\_TPM\_GetRandom command, 195

Tspi\_TPM\_KeyControlOwner command,  
284-285

Tspi\_TPM\_KillMaintenanceFeature  
command, 237

Tspi\_TPM\_ReadCurrentCounter  
command, 275

Tspi\_TPM\_ReadCurrentTicks command, 276

Tspi\_TPM\_RevokeEndorsementKey  
command, 280-281

Tspi\_TPM\_SetOrdinalAuditStatus  
command, 273

Tspi\_TPM\_TickStampBlob command,  
276-277

TSS (Trusted Computing Group Software  
Stack), 77

- commands, 303-313
- design, 77-79, 94-102
- functions, 323-331
- PKCS#11. *See* PKCS#11

TSS Core Service. *See* TCS

TSS\_buildbuff() function, 65

TSS\_Data\_Bind command, 195

TSS\_Data\_Unbind command, 195

TSS\_TPMSTATUS\_MAINTENANCEUSED  
flag, 237

types element, 148

## U-V

upgrading, 231

usage models, 21

users

- isolation of, 23-24
- multiple, 213

utility functions, keys, 104, 107

utilization, TCS, 145-152

validation data structure, TSS, 101-102

Verified by VISA protocol, 212

verifying data, 97-99

virtual dongles, 221

virtual private networks. *See* VPNs

viruses, 7

VOIP (voice over IP), 207

VPNs (virtual private networks), 208-210,  
226-227

vulnerable programs, 5-6

## W-Z

water usage service meters, 227-228

writing

- code, 145
- TPM device drivers, 45-58

WSDL (Web Services Description Language),  
145-152





















# THIS BOOK IS SAFARI ENABLED

## INCLUDES FREE 45-DAY ACCESS TO THE ONLINE EDITION

The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days.

Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

### **TO GAIN 45-DAY SAFARI ENABLED ACCESS TO THIS BOOK:**

- Go to <http://www.awprofessional.com/safariabled>
- Complete the brief registration form
- Enter the coupon code found in the front of this book on the "Copyright" page

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail [customer-service@safaribooksonline.com](mailto:customer-service@safaribooksonline.com).



Addison  
Wesley