

Standards that define ciphersuites

Stefan Schumacher <public@cryptomancer.de>

Table of Contents

1. Taxonomy Dimensions	1
1.1. Braindump list	1
1.2. Taxonomy Categories (1st Level)	3
1.2.1. German BSI	3
1.2.2. USA NIST	4
1.2.3. Attributes	4
1.3. Protocols	5
1.3.1. Protocols with Implementations	5

- compiled at 2026-04-18 16:20:44 +0200 Version 0.0.1 of 2026/04/17, draft
- **Datei:** Standards

Scope: This document will list all standards that define the properties of ciphersuites (algorithm, key length, mode) etc. The aim is to generate an exhaustive list of cryptographic material to be used as a database for CBOMs.

1. Taxonomy Dimensions

1.1. Braindump list

Braindump

1. Status
 - a. Approved
 - b. Obsolete / Deprecated
 - c. Legacy
 - d. Broken
2. Protocols
 - a. TLS
 - i. TLS 1.3
 - ii. TLS 1.2
 - iii. TLS 1.1
 - iv. TLS 1.0
 - v. SSL 3

- vi. SSL 2
 - b. Secure Shell
 - i. SSH1 (deprecated)
 - ii. SSH2
 - A. OpenSSH
 - B. Dropbear
 - C. SSH Tectia Client/Server
 - c. Internet Key Exchange IKE
 - i. IKEv1
 - ii. IKEv2
 - d. PPTP
 - e. Radius
 - f. MS-CHAP
 - g. IPSec
 - i. OpenVPN
 - ii. FreeSWAN/StrongSWAN
 - iii. Wireguard
 - h. Online Certificate Status Protocol
 - i. OpenPGP
 - i. LibrePGP
 - ii. GnuPG
 - iii. age
 - j. Kerberos
 - k. JWT
 - i. JOSE
 - l. FIDO2 Passkeys
- 3. .PKI
 - i. X.509
 - ii. Cryptographic Message Syntax
 - 4. Symmetric
 - 5. Asymmetric
 - 6. Key Exchange
 - 7. Key Length
 - a. 56, 128, 196, 256
 - 8. Operation Mode
-

- a. Streamcipher
- b. Blockcipher
- c. Electronic Codebook Mode (ECB)
- d. Cipher Block Chaining Mode (CBC)
- e. Counter Mode (CTR)
- f. Galois Counter Mode (GCM)
- g. XOR-Encrypt-XOR (XEX)
- h. XEX-based Tweaked-Codebook mode with ciphertext stealing (XTS)
- i. Synthetic Initialization Vector (SIV)
- j. Encrypt Mix Encrypt (EME)
- k. Cipher Feedback Mode (CFB)
- 9. IANA CipherSuite
- 10. Hash
 - a. Message Authentication Code (MAC)
 - b. HMAC
- 11. PQC
- 12. PQC-Hybrid
- 13. One Time Password (OTP)
 - a. Hash based OTP
 - b. Time based OTP
- 14. Cryptographically Secure Pseudorandom Number Generator (CSPRNG)
 - a. Dual_EC_DRBG
- 15. WIFI
 - a. WEP
 - b. WPA
 - c. WPA2
 - d. WPA3

1.2. Taxonomy Categories (1st Level)

1.2.1. German BSI

Sources:

1. BSI TR-02102-x (Kryptographische Verfahren: Empfehlungen und Schlüssellängen)
2. BSI AIS 20/31 (A proposal for: Functionality classes for random number generators - Version 3.0)
3. BSI TR-03116

4. BSI TR-03111 Elliptic Curve Cryptography, Version 2.10

- Asymmetric Algorithms
 - Digital Signature
 - Key Exchange
- Symmetric Algorithms
- Hash Functions
- Message Authentication Codes (MACs)
- Random Number Generators

1.2.2. USA NIST

sources:

1. NIST SP 800-57
2. NIST SP 800-56A - KEX
3. NIST FIPS 186-5 - Signatures
4. NIST SP 800-38 - Symmetric
5. NIST SP 800-185 - Hash/KDF
6. NIST SP 800-90A - RNG
7. NIST SP 800-208 - PQC Signatures
 - Key Exchange / Key Establishment
 - Public-Key Encryption
 - Digital Signatures
 - Symmetric Encryption
 - Hash Functions
 - MAC / AEAD
 - Key Derivation Functions (KDFs)
 - Random Number Generation

1.2.3. Attributes

1. Protocol
2. Library/Program/Implementation
 - a. Version
3. State
 - a. Data at rest
 - b. Data in transit
 - c. Data in Use

1.3. Protocols

- TLS (Transport Layer Security)
- SSH (Secure Shell)
- IPsec (Internet Protocol Security)
- HTTPS (HTTP over TLS)
- DTLS (Datagram Transport Layer Security)
- QUIC (Quick UDP Internet Connections)
- OpenPGP
- S/MIME (Secure/Multipurpose Internet Mail Extensions)
- Kerberos
- Wireless Security
- VPN
- PKI
- Certificates
- Messaging security protocols
- File encryption
- Storage encryption

1.3.1. Protocols with Implementations

1. TLS (Transport Layer Security)
 - a. TLS 1.2
 - b. TLS 1.3
2. SSH (Secure Shell)
 - a. SSHv2
 - b. SFTP
 - c. SCP
3. IPsec (Internet Protocol Security)
 - a. IKEv1
 - b. IKEv2
 - c. ESP
 - d. AH
4. HTTPS (HTTP over TLS)
5. DTLS (Datagram Transport Layer Security)
6. QUIC (Quick UDP Internet Connections)

- a. HTTP/3 over QUIC
- 7. OpenPGP
- 8. S/MIME (Secure/Multipurpose Internet Mail Extensions)
- 9. Kerberos
 - a. Kerberos v5
- 10. Wireless Security
 - a. WPA3
 - b. WPA2
- 11. VPN
 - a. OpenVPN
 - b. WireGuard
 - c. L2TP
 - d. IPsec
- 12. PKI
 - a. X.509
- 13. Certificates
 - a. OCSP (Online Certificate Status Protocol)
 - b. CRL (Certificate Revocation List)
- 14. Messaging security protocols
 - a. Matrix MegOlm
 - b. Matrix MLS
 - c. Signal
 - d. Threema
 - e. WhatsApp
 - f. XMPP
 - i. Off-the-Record
 - ii. Omemo
 - iii. OpenPGP over XMPP
 - iv. S/MIME
 - v. Jingle && DTLS-SRTP
- 15. File encryption
- 16. Storage encryption