

Standards that define ciphersuites

Stefan Schumacher <public@cryptomancer.de>

Table of Contents

1. Taxonomy Dimensions	1
------------------------------	---

- compiled at 2026-04-17 20:26:26 +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. Status

- a. Approved
- b. Obsolete / Deprecated
- c. Legacy

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. IPSec
 - i. OpenVPN
 - ii. FreeSWAN/StrongSWAN
 - iii. Wireguard
- e. Online Certificate Status Protocol
- f. OpenPGP
 - i. LibrePGP
 - ii. GnuPG
 - iii. age
- g. Kerberos
- h. JWT
 - i. JOSE
- i. 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
- 9. IANA CipherSuite
- 10. Hash
 - a. MAC
- 11. PQC
- 12. PQC-Hybrid