# Network Security

Table of Contents



## Abbrevations

### A

- AAD: Associated Authenticated Data [Crypto]
- AD: Active Directory [IAM]
- Auth**N**: Authe**n**tication [Auth]
- Auth**Z**: Authori**z**ation [Auth]
- ACME: Automatic Certificcate Management Environment [Certificate]
- AEAD: Authenticated Encryption with Associated Data [Crypto]
- AES: Advanced Encryption Standard [Crypto]
- AH: Authentication Header [VPN]
- ALPN: Application Layer Negotiation Protocol [TLS]

### C

- CA: Certificate Authority [Certificate]
- CBC: Cipher-Block-Chaining-Mode [Crypto]
    - CCM: Counter-Mode with Cipher-Block-Chaining Message Authentication Code [Crypto]
- CFB: Cipher Feedback Mode [Crypto]
- CHAP: Challenge Handshake Authentication Protocol [Auth]
- CN: Common Name [Certificate]
- CRAM-MD5: Challenge Response Authentication Mechansim, Message Digest 5 [Crypto]

- CSR: Certificate Signing Request [Certificate]
- CTAM: Client to Authenticator Protocol [FIDO]
- CTR: Counter Mode [Crypto]
  - CCM: Counter Mode with CBC-MAC [Crypto]

**D**

- DANE: DNS-based Authentication of Named Entities [TLS]
- DES: Data Encryption Standard [Crypto]
- DH: Diffie-Hellman [Crypto]
- DLP: Discrete Logarithm Problem [Crypto]
- DNS: Domain Name System [TLS]
  - DNSSEC: Domain Name System Security Extensions [TLS]
- DoH: DNS over HTTPS [TLS]
- DoS: Denial of Service [Attack]
  - DDoS: Distributed Denial of Service [Attack]
- DSA: Digital Signature Algorithm [Crypto]
- DTLS: Datagram Transport Layer Security [TLS]
- DV: Domain-validated [Certificate]

**E**

- EAP: Extensible Authentication Protocol [Auth]
- ECB: Electronic Codebook Mode [Crypto]
- ECC: Elliptic Curve Cryptography [Crypto]
  - ECDH: Diffie-Hellman with Elliptic Curves [Crypto]
  - ECDSA: Elliptic Curve Signature Algorithm [Crypto]
- ED25519: Edwards Curve 25519 [Crypto]
- ESP: Encapsulating Security Payload [VPN]
- ETH: Ethernet
- EV: Extended validation [Certificate]

**F**

- FIDO: Fast Identity Online [Auth]
- FIPS: Federal Information Processing Standard [Crypto]
- FQDN: Fully Qualified Domain Name [TLS]
- FTP: File Transfer Protocol [TLS]
  - FTPS: File Transfer Protocol over TLS [TLS]

**G**

- GCM: Galois Counter Mode [Crypto]
- GPG: GNU Privacy Guard
- GSSAPI: Generic Security Service Application Programming Interface [Auth]

**H**

- HMAC: Hashed Message Authentication Code [Crypto]
- HOTP: HMAC-based One-Time Password [MFA]
- HSTS: HTTP Strict Transport Security [TLS]
- HTTP: Hypertext Transfer Protocol
  - HPKP: HTTP Public Key Pinning [TLS]
  - HTTPS: Hypertext Transfer Protocol Secure

**I**

- ICV: Integrity Check Value [Crypto]
- ID: Identity
- IEEE: Institute of Electrical and Electronics Engineers
- IETF: Internet Engineering Task Force
- IKE: Internet Key Exchange [VPN]
- IP: Internet Protocol

  - IPv4: Internet Protocol version 4
  - IPv6: Internet Protocol version 6
  - IPSec: Internet Protocol Security [VPN]
- IV: Initialization Vector [Crypto]

**J**

- JWT: JSON Web Token [OAuth]

**K**

- KDC: Key Distribution Center [IAM]
- KPA: Known-plaintext Attack [Attack]
- KSK: Key Signing Key

**L**

- LAN: Local Area Network
- LDAP: Lightweight Directory Access Protocol [IAM]
- L1/L2/L3: Layer 1/2/3

**O**

- OAUTH: Open Authorization [IAM]
  - OIDC: OpenID Connect [IAM]
- OFB: Output Feedback Mode [Crypto]
- OCSP: Online Certificate Status Protocol [Certificate]
- OTP: One-Time Password [MFA]
  - TOTP: Time-based One-Time Password [MFA]
  - HOTP: HMAC-based One-Time Password [MFA]
- OV: Organization-validated [Certificate]

**M**

- MAC: Message Authentication Code [Crypto]
  - Synonyms:
    * MIC: Message Integrity Code
    * MDC: Modification Detection Code
    * ICV: Integrity Check Value
  - Variants:
    * CBC-MAC: Cipher Block Chaining Message Authentication Code
    * GMAC: Galois Message Authentication Code
    * HMAC: Hashed Message Authentication Code
- MFA: Multi-factor Authentication [Auth]
- MIME: Multipurpose Internet Mail Extensions [Mail]
  - S/MIME: Secure Multipurpose Internet Mail Extensions
- MITM: Man-in-the-Middle [Attack]
- MTA: Mail Transfer Agent [Mail]
  - MTA-STS: Mail Transfer Agent Strict Transport Security

**N**

- NAT: Network Address Translation [VPN]
- NIST: National Institute of Standard and Technology

**P**

- P2P: Peer-to-Peer [VPN]
- PAP: Password Authentication Protocol [Auth]
- PFS: Perfect Forward Secrecy [Crypto]
- PGP: Pretty Good Protection [WoT]
  - GPG: GNU Privacy Guard
- PKCE: Proof Key for Code Exchange

- PKC: Public Key Cryptography [Crypto]
- PKI: Public Key Infrastructure [Certificate]
- PPP: Point-to-Point Protocol
- PRF: Pseudo Random Function

**R**

- RADIUS: Remote Authentication Dial-In User Service [Auth]
- RNG: Random Number Generator
  - PRNG: Pseudo-random Number Generator
- RP: Replying Party
- RR: Round-Robin, Resource Record [DNS]
- RSA: Rivest, Shamir, Adleman-Algorithm [Crypto]
- RTC: Real-Time Communication

**S**

- SA: Security Association [IPSec]
  - SAD: Security Association Database [IPSec]
- SAD: Security Association Database [IPSec]
- SAML: Security Assertion Markup Language
- SAN: Subject Alternative Name [TLS]
- SASL: Simple Authentication and Security Layer [Auth]
- SCRAM: Salted Challenge Response Authentication Mechanism [Auth]
- SHA: Secure Hash Algorithm
- S/MIME: Secure Multipurpose Internet Mail Extensions [Mail]
- SMTP: Simple Mail Transfer Protocol [Mail]
  - SMTPS: Simple Mail Transfer Protocol over TLS [TLS]
- SNI: Server Name Indication [TLS]
  - ESNI: Encrypted Server Name Indication [TLS]
- SOCKS: Sockets
- SP: Security Policy [IPSec]
  - SPD: Security Policy Database [IPSec]
- SSH: Secure Shell
- SSL: Secure Socket Layer [TLS]
  - TLS: Transport Layer Security
- SSO: Single Sign-on

**T**

- TAN: Transaction Authentication Number [MFA]
- TCP: Transport Control Protocol
- TGT: Ticket Granting Ticket Kerberos
- TLD: Top-level Domain [DNS]
- TLS: Transport Layer Security [TLS]
  - DTLS: Datagram Transport Layer Security [TLS]
  - TLSA: Transport Layer Security Association [TLS]
  - TTLS: Tunneled Transport Layer Security [TLS]
- TOFU: Trust-on-first-use [TLS]
- TOTP: Time-based One-Time Password [MFA]

**U**

- UDP: User Datagram Protocol
  - DTLS: Datagram Transport Layer Security

**V**

- VPN: Virtual Private Network

**W**

- WEP: Wired Equivalent Privacy [Auth]

- Wi-Fi: Wireless Fidelity
- WLAN: Wireless Local Area Network
- WoT: Web of Trust
- WPA: Wi-Fi Protected Access [Auth]
- WPS: Wi-Fi Protected Setup [Auth]

### Z

- ZSK: Zone Signing Key

## Definitions

- **Authentication / Authentifizierung**: eine Person ist authentifiziert, wenn ihre Identität festgestellt werden konnte. Das kann mithilfe von Passwörtern, Biometrischen Daten oder einfach dem Ausweis erfolgen. Authentifizierung hängt mit Authorization zusammen, da man Berechtigungen nach Personen(gruppen) vergeben möchte.
- **Authorization / Autorisierung**: die Berechtigung eine Aktion tun zu dürfen oder auf eine Ressourcen zugreifen zu dürfen.
- **Confidentiality / Vertraulichkeit**: der Inhalt einer Nachricht ist mithilfe von Verschlüsselung für dritte nicht mehr lesbar.
- **Diffusion**: eine Verschlüsselungsoperation, bei der der Einfluss eines Klartexts auf den Cipher gestreut wird, um statistische Eigenschaften des Klartexts zu verbergen. *Eselsbrücke*: Diffuse = Verteilen
- **Konfusion**: eine Verschlüsselungsoperation, die die Beziehung zwischen Schlüssel und Cipher verschleiert. Dafür werden Substitutionstabellen verwendet, die in DES und AES verwendet werden. *Eselsbrücke*: Confuse = Verwirren
- **Integrity / Integrität**: der Inhalt einer Nachricht kann nicht unbemerkt modifiziert werden.
- **Non-Repudiation**: eine Partei kann nicht mehr abstreiten, dass sie eine Nachricht tatsächlich gesendet hat. Das wird vor allem mit Zertifikaten sichergestellt.
- **Safety**: Schutz vor Verlust von Daten, etwa durch Hardwarefehler.
- **Security**: Schutz vor unautorisiertem Zugriff, etwa auf private Informationen.

## Links

### Certificates

- How does HTTPS work? What's a CA? What's a self-signed Certificate?: https://www.youtube.com/watch?v=T4Df5_cojAs
- Digital Certificates Explained * How digital certificates bind owners to their public key: https://www.youtube.com/watch?v=5rT6fZUwhG8
- CA/Terminology: https://wiki.mozilla.org/CA/Terminology

### Authentication and Authorization

### Multifactor Authentication

### Lamport

- Example of how Lamport OTP work: https://www.infoworld.com/article/2078022/lamport-s-one-time-password-algorithm--or--don-t-talk-to-complete-strangers--.html?page=2
- Difference between Lamport OTP and HOTP and TOTP: https://security.stackexchange.com/a/90910

### Identity Management

### Kerberos

- Kerberos Authentication Explained: https://www.youtube.com/watch?v=5N242XcKAsM

### OAuth 2.0 and OIDC

- OAuth 2.0 and OpenID Connect: https://www.youtube.com/watch?v=996OiexHze0

### VPN + IPSec

#### Modes and Protocols

- AH - Authentication Header: https://www.elektronik-kompendium.de/sites/net/1410251.htm
- ESP - Encapsulating Security Payload: https://www.elektronik-kompendium.de/sites/net/1410261.htm
- IPsec Tunnel Mode vs. Transport Mode: https://www.twingate.com/blog/ipsec-tunnel-mode
- Security Association Database (IPv6 and IP Security): https://what-when-how.com/ipv6-advanced-protocols-implementation/security-association-database-ipv6-and-ip-security/