# Abkürzungsverzeichnis Netzsicherheit

| Akronym | Kontext | Erläuterung |
|---|---|---|
| AA | Zertifikate | Authentication Authority |
| AAA | | Authentication, Authorisation, Accounting |
| ACL | | Access Control List |
| ACRL | Zertifikate | Attribute CRL |
| AES | Kryptographie | Advanced Encryption Standard |
| AH | IPsec | Authentication Header |
| ARP | Grundlagen | Address Resolution Protocol |
| AS | Netzzugang | Authentifizierungsserver, |
| AS_REP | Kerberos | Authentification Server Reply |
| AS_REQ | Kerberos | Authentification Server Request |
| ASN.1 | Kodierung | Abstract Syntax Notation |
| ASO | Organisation | Address Supporting Organisation |
| ATM | Grundlagen | Asynchron Transfer Modus |
| BER | Kodierung | Basic Encoding Rules |
| CA | Zertifikate | Certification Authority |
| CAP(-Prinzip) | Zertifikate | Consistency, high Availibility, partition-resilence |
| CARL | Zertifikate | Certification Authority Revokation List |
| CBC | Kryptographie | Cipher-Block-Chaining |
| CCP | | Compression Control Protocol, RFC 1962 |
| CHAP | Netzzugang | Challenge Handshake Authentication Protocol |
| CMP | | Certificate Management Protocol |
| CMS | | Certificate Management Messages, Cryptographic Message Syntax |
| CRC | Grundlagen | Cyclic Redundancy Check |
| CRL | Zertifikate | Certificate Revokation List |
| CRLDP | Zertifikate | CRL Distribution Point |
| CRMF | Zertifikate | Certifcate Management Request Format |
| DAC | | Discretionary Access Control |
| dCRL | Zertifikate | Delta-CRL |
| Ddos | Angriff | Distributed Denial of Service (Distributed Dos) |
| DER | Kodierung | Distinguished Encoding Rules |
| DES | Kryptographie | Data Encryption Standard |
| DH | Kryptographie | Diffie-Hellman |
| DHCP | Grundlagen | Dynamic Host Control Protocol |
| DOS | Angriff | Denial of Service |
| DSL | Grundlagen | Digital Subscriber Line |
| EAP | Netzzugang | Extensible Authentication Protocol (RFC 2284) |
| EAP-TLS | Netzzugang | RFC 2716 |
| EAP-TTLS | Netzzugang | EAP Tunneled TLS Authentication Protocol |
| ECB | Kryptographie | Eletronic Code Block |
| ECP | Netzzugang | Encryption Control Protocol (RFC 1968) |
| EPRL | Zertifikate | End-entity Public-key |
| ESP | IPsec | Encapsulating Security Payload |
| GCM | Kryptographie | Galois/Counter Mode |
| GTK | | Group Transient Key |

| | | |
|---|---|---|
| HDLC | Grundlagen | High Level Data Link Control |
| HMAC | Kryptographie | Hash MAC |
| ICMP | Grundlagen | Internet Control Message Protocol |
| iCRL | Zertifikate | Indirect CRL |
| ICV | Kryptographie | Integrity Check Value |
| IDS | | Intrusion Detection Software |
| IETF | Organisation | Internet Engeneering Taskforce |
| IKE | IPsec | Internet Key Exchange |
| IMAP | Mail | Internet Mail Access Protocol |
| IP | Grundlagen | Internet Protocol |
| ISAKMP | IPsec | Internet Security Association and Key Management Protocol |
| ISDN | Grundlagen | Integrated Services Digital Network |
| ISO/OSI | Organisation | Internation Organisation for Standardization |
| IV | Kryptographie | Initialisierungsvektor |
| KCK | | Key Confirmation Key (128 Bit) |
| KDC | Kerberos | Key Distribution Center (=AS+TGS) |
| KEK | | Key Encryption Key (128 Bit) |
| LCP | Netzzugang | Link Configuration Protocol |
| LLC | Grundlagen | Logical Link Control |
| LZW | Kodierung | Lempel-Ziv-Welch |
| MAC | Kryptographie | Message Authentication Code<br>Mandatory Access Control |
| MIME | Mail | Multipurpose Internet Mail Extension |
| MRU | | Maximum Receive Unit |
| MTA | Mail | Mail Transfer Agent |
| MTI | Mail | Meter TI |
| NAS | Netzzugang | Network Access Server |
| NCP | Netzzugang | Network Configuration Protocol |
| NFS | Grundlagen | Network File System |
| OCSP | Zertifikate | Online Certificate Status Protocol |
| OID | | Object Identifier |
| OTP | Kryptographie | One Time Pad, RFC 2289 |
| PADI | Netzzugang | PPPoE Discovery Initiation |
| PADO | Netzzugang | PPPoE Active Discovery Offer |
| PADR | Netzzugang | PPPoE Active Discovery Request |
| PADS | Netzzugang | PPPoE Active Discovery Session confirmation |
| PADT | Netzzugang | PPPoE Active Discovery Termination |
| PAE | | Port Access Entities |
| PAP | Netzzugang | Password Authentication Protocol, RFC 1334 |
| PCBC | Kerberos | Plaintext CBC |
| PEAP | Netzzugang | Protected EAP |
| PERMIS | Zertifikate | Privilege and Role Management Infrastructure Standards |
| PFS | Kryptographie | Perfect Forward Secrecy |
| PGP | Mail | Pretty Good Piracy |
| PKCS | | Public Key Cryptography Standards |
| PKI | Zertifikate | Public Key Infrastructure |
| PKK | Kryptographie | Public Key Kryptographie |
| PMI | Zertifikate | Priviledged Management Infrastructure |
| POP | Mail | Post Office Protocol |
| PPP | Netzzugang | Point-to-Point Protocol, RFC 1661 |

| | | |
|---|---|---|
| PPPoE | Netzzugang | PPP over Ethernet |
| PRF | Kryptographie | Pseudo Random Function |
| PTK | | Pairwise Timeout Key |
| PtP | Netzzugang | Punkt-zu-Punkt Verbindungen |
| QOS | Grundlagen | Quality of Service |
| RA | Zertifikate | Registration Authority |
| RADIUS | Netzzugang | Remote Authentification Dial In User Service, RFC 2138 |
| R-bac | | Role based Access Control |
| RSVP | Grundlagen | Resource ReSerVation Protocol, RFC 2205 |
| S/KEY | | RFC 1760 |
| S/Mime | Mail | Secure Mime |
| SAD | IPsec | Security Association Dataframe |
| SCVP | Zertifikate | Simple Certificate Validation Protocol |
| SLIP | Einwahl | Serial Line IP, RFC 1055 |
| SMTP | Mail | Simple Mail Transport Protocol |
| SNMP | | Simple Network Management Protocol |
| SOA | Zertifikate | Source of Authority |
| SPD | IPsec | Security Policy Database |
| SPI | IPsec | Security Parameter Index |
| SSH | | Secure Shell |
| SSL | TLS | Secure Socket Layer |
| StK | | String to Key |
| TGS | Kerberos | Ticket-Granting-Server |
| TGT | Kerberos | Ticket-Granting-Ticket |
| TI | Mail | Trust Introducer |
| TLS | TLS | Transport Layer Security |
| TLSE | TLS | TLS-Extensions, RFC 3546 |
| TLV | Kodierung | Type-Length-Value |
| UDP | Grundlagen | User Datagram Protocol |
| WEP | Netzzugang | Wired Equivalent Privacy |
| WPA | Netzzugang | Wi-fi Protected Access |
| X.509 | Zertifikate | RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile |