

Inhaltsverzeichnis

1. Sicherheit, DSG, Symmetrische und Asymmetrische Verschlüsselung
2. Signaturen, Zertifikate, Identität, Identifikation, Authentifizierung, Autorisierung, Angriffe, Verzeichnisdienste, LDAP
3. PKI-Komponenten, Elektronische Signatur, Zertifikate, HSM, PSE, TSA, PKCS (Public Key Cryptographic Standards), Zertifikatserzeugungs- und Signierungsantrag (CSR)
4. ASN.1, Transfersyntax (BER)
5. X.509 Zertifikate, Qualifiziertes Zertifikat, Attribut Zertifikat, Zertifikatspfad
6. Risiken bei Applikationen mit Zertifikaten, Extended Validation Zertifikate
6.1 PKCS#10 Zertifizierungsanfrage
7. Sperrlisten (CRL)
8. Verzeichnisdienst (OCSP)
9. Trustketten und Prüfung der Zertifikate, Gültigkeitsmodelle
10. Zeitstempeldienst
11. Hash-Funktionen
12. Keyed-Hash Message Authentication Code (HMAC)
13. SSL / TLS, Record-Protokoll, Handshake-Protokoll, Change Cipher Spec Protokoll, Alert Protokoll, Applicationkryptographische Komponenten von Data Protocoll, SSL / TLS, Unterschiede SSL / TLS, Angriffe gegen SSL / TLS
14. IPsec
 - Übertragungsmodi
 - Teilprotokolle
 - Authentication Header
 - Encapsulated Security Payload
 - IPsec-Management (SA, SPD, ISAKMP, Oakley)
 - IKEv1
 - IKE Quick Mode
 - NAT-Traversal
 - IKEv2
 - Unterschiede IKEv1 / IKEv2
15. Kerberos
16. Chipkarten
 - Dateiverwaltung
 - Basic interindustry commands
 - Java Cards