



Risicomanagement

Te beschermen belangen | Dreigingen / actoren / motivaties | Risico's | Compliance



Informatiebeveiliging doelen

Beschikbaarheid | Integriteit | Vertrouwelijkheid | Authenticiteit | Onweerlegbaarheid



Cryptografische functionaliteiten

Ondertekenen | Versleutelen | Authentifieren | Sleuteluitwisseling | Dataverificatie

Implementatie requirements



Implementatie

Cryptografische Standaard | Library | Mechanisme | Protocol | Parameters | Suite | Algoritme

Bouwblokken voor



Cryptografische primitieven

Symmetrische encryptie | Asymmetrische encryptie | Random number generation |
(Cryptografische) hashfunctie | Digitale handtekening | MAC (message-authentication code) |
Sleutelaflleiding (key derivation) | Sleuteldistributie (key distribution)