# **Digitale Handtekening**

Op het examen duidelijk zeggen welke Key ge gebruikt (prive/public) en van wie (persoon A of B).

Je gaat een MD5-hash (128-bit getal) (fingerprint) doorsturen door een RSA met de privé key van u eigen, dan krijg je je digitale handtekening.

MD5 🡪 RSA met eigen key 🡪 handtekening

Hybride Crypto

Symmertisch (AES)

Positief: snel

Negatief: Key management

Assymetrisch (RSA)

Positief: Weinig key management

Negatief : traag

Hash

Fingerprint , D.S

EXAMEN Hoe groot is de DES sleutel (64 bit , 8 controle bits)

Certificaten

-ID

-Public Key

Comodo certificcaat bv.

Bedrijf : CA 🡪 die encryteerd dat met zijn eigen privé key.

X.509 v3 certificaten

Waarom vertrouw je een certificaat:

Kopen bij een bedrijf , een CA. Dat bedrijf signed dat bestand , als je dat certificaat wilt decrypteren, heb je de public key nodig. Boomstructuur , IS gebaseerd dus op vertrouwen.

Root certificaat iss hard-coded in de browser

Een ganse keten van CA’s , tot een RootCA , als je dan den RootCA hackt , valt alles uit.

Grootste DDos attack , 9/11 , iedereen googelede iedereen dat filmke van CNN die live bezig waren , teveel requesten over heel de wereld , crash van internet voor een hele dag.

PKI (public key infrastructere )

Leg me uit wat de verschillende componenten zijn van een PKI bedrijfke (**Examen**).

Proof Of Posession controleren: klein bestande encrypteren met die public key, decrypteer nu eens met die Private key. Kom je dat bestand uit dan heb je PoP bewezen.

Nadat je dat certificaat gemaakt is (door RA) dan stop je dat in een Database(DB)

Certification Revocation List. Dat is de blacklist van certificaten 🡪 certificaten die je niet meer mag vertrouwen.

Certificaat wordt gemaakt door x.509 v3.

Certification Policies en Certification Practice statements, dat bedrijf gaat in documenten moeten zetten hoe ze certificaten maken.

CP = soort certificaat dat ze maken

CPS = hoe ze dat gaan maken bv: DNA , AES , RSA (2048 key length) , SHA-2.

Dit gaan ze bij houden in een database.

Welk protocol wordt gebruikt om certificaten te controleren:

Validation Authority.

OCSP = Online Cerfication Status Protocol. 🡪 server met alle black nog iets die voor u gaat checken of dat certificaat klopt.

**HOE?**

Nu is het een single point of failure , en ze willen gaan naar een Mesh structuur 🡪 cross certificering

Verisign had een Masieve CRL (Blacklist) 🡪 dus ge ging dan vragen of da effectief een goei certificaat was. 🡪 database te groot duurt da te lang. 🡪 dus ze gaan load balancing doen door meerdere servers te hebben , OCSP servers 🡪 connectie 1 gaat naar server 1 , connectie 2 naar server 3,…. 🡪 is veel sneller .

**Key Escrow:**

Uw private key aan een bedrijf geven voor beheer voor als je iets mis doet. 🡪 Als je een programma gebruikt dat te goed geyncrepteerd is dat zelfs NSA niet kan decrypteren.

**HOOFDVRAAG EXAMEN:**

Wat zijn de verschillende componenten van de PKI , wat is de RA, CA , CRL , CP , CPS , VA