Cryptografie: ontwikkelingen en valkuilen bij gebruik

Eric Verheul

Bart Jacobs

5 oktober 2011

Radboud Universiteit Nijmegen

Digital Security group

Agenda

- Context
- Verbeter suggesties HSM opzet binnen CSPs (langere termijn)
- Verbeter suggesties HSM opzet binnen CSPs (kortere termijn)
- Verbeterde technische monitoring via nieuw type HSM
- Afsluiting

Context

- Cryptografie is de wetenschap van het beschermen van de vertrouwelijkheid, en/of integriteit van informatie met wiskundige methoden.
- Cryptanalyse is de wetenschap van het aanvallen van de cryptografische bescherming middels wiskundige methoden.

Context

Aanvallen:

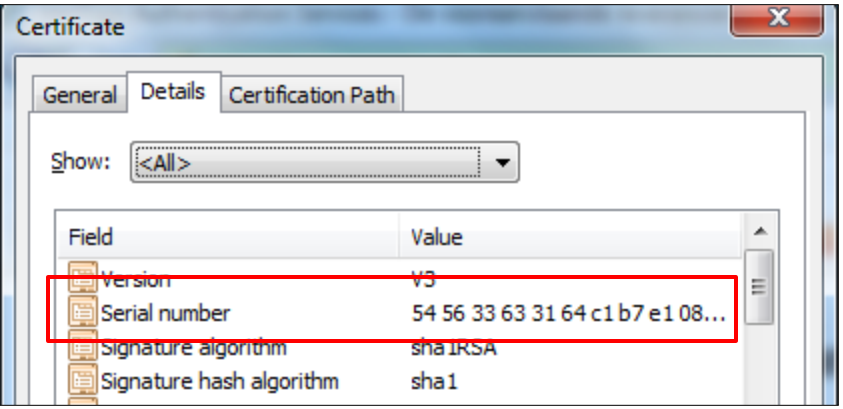
- Cryptanalyse / te korte sleutellengten
- Zelf ontwikkelde cryptografische algoritmen
- Verkeerd gebruik van op zich goede cryptografische algoritmen
- Omzeilen van de cryptografische beveiliging

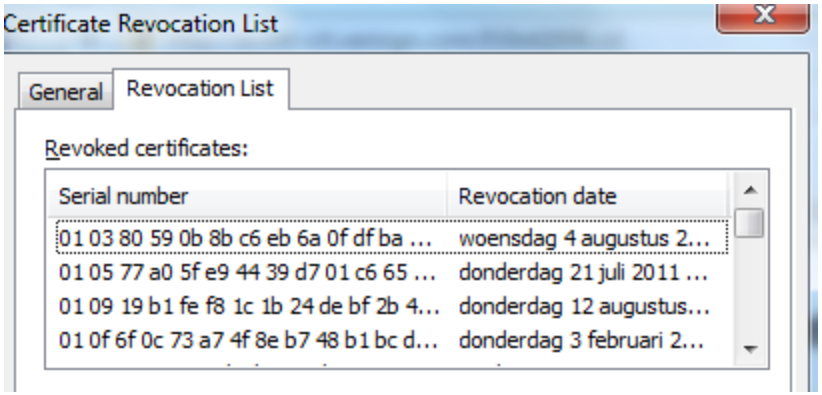
Context

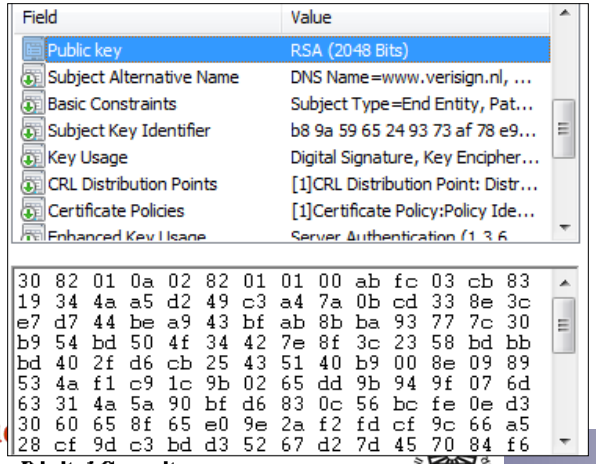
Cryptografie in de praktijk: SSL/TLS

SSL certificaten: publieke sleutels verpakt in een getekend certificaat

Certificate Revocation List (CRL): registratie van ingetrokken certificaten op basis serial number



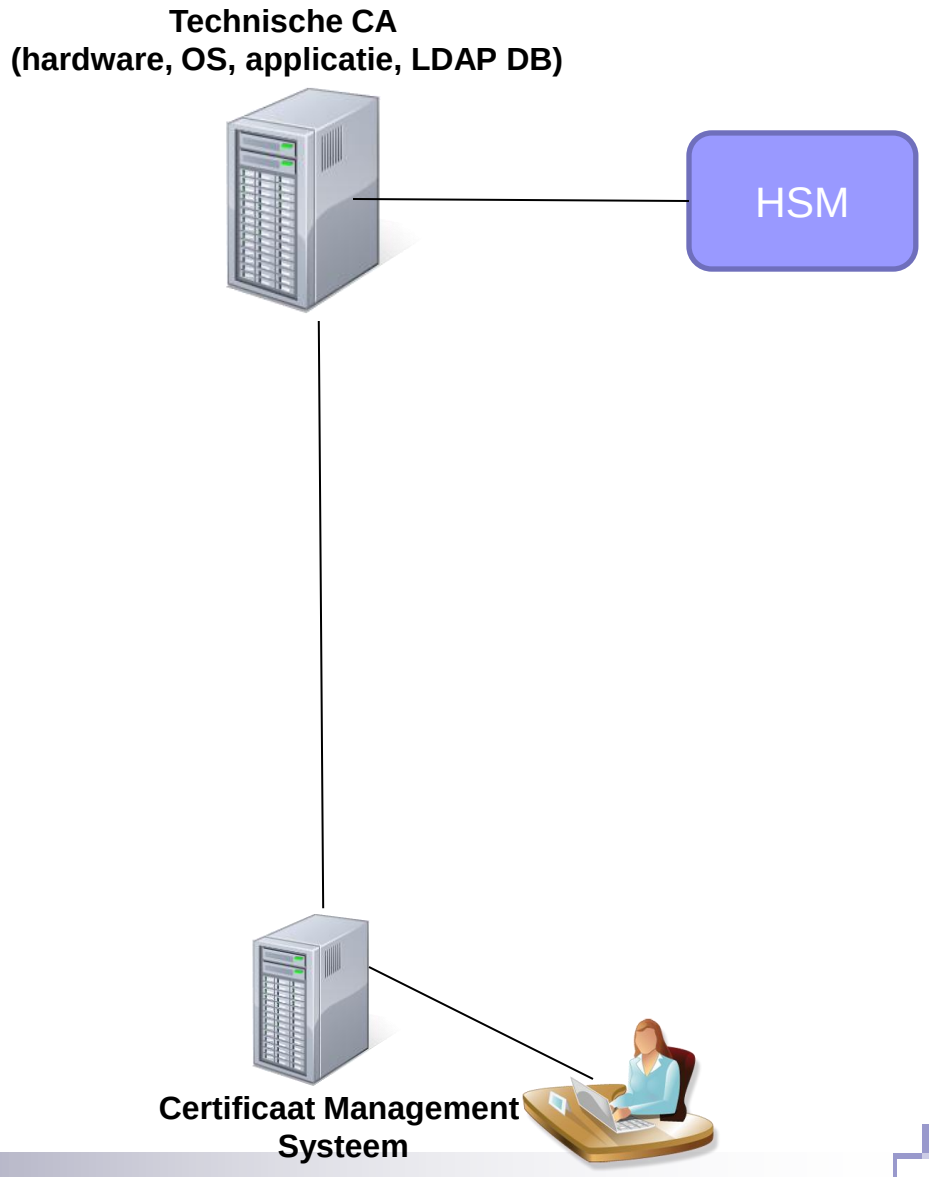




Agenda

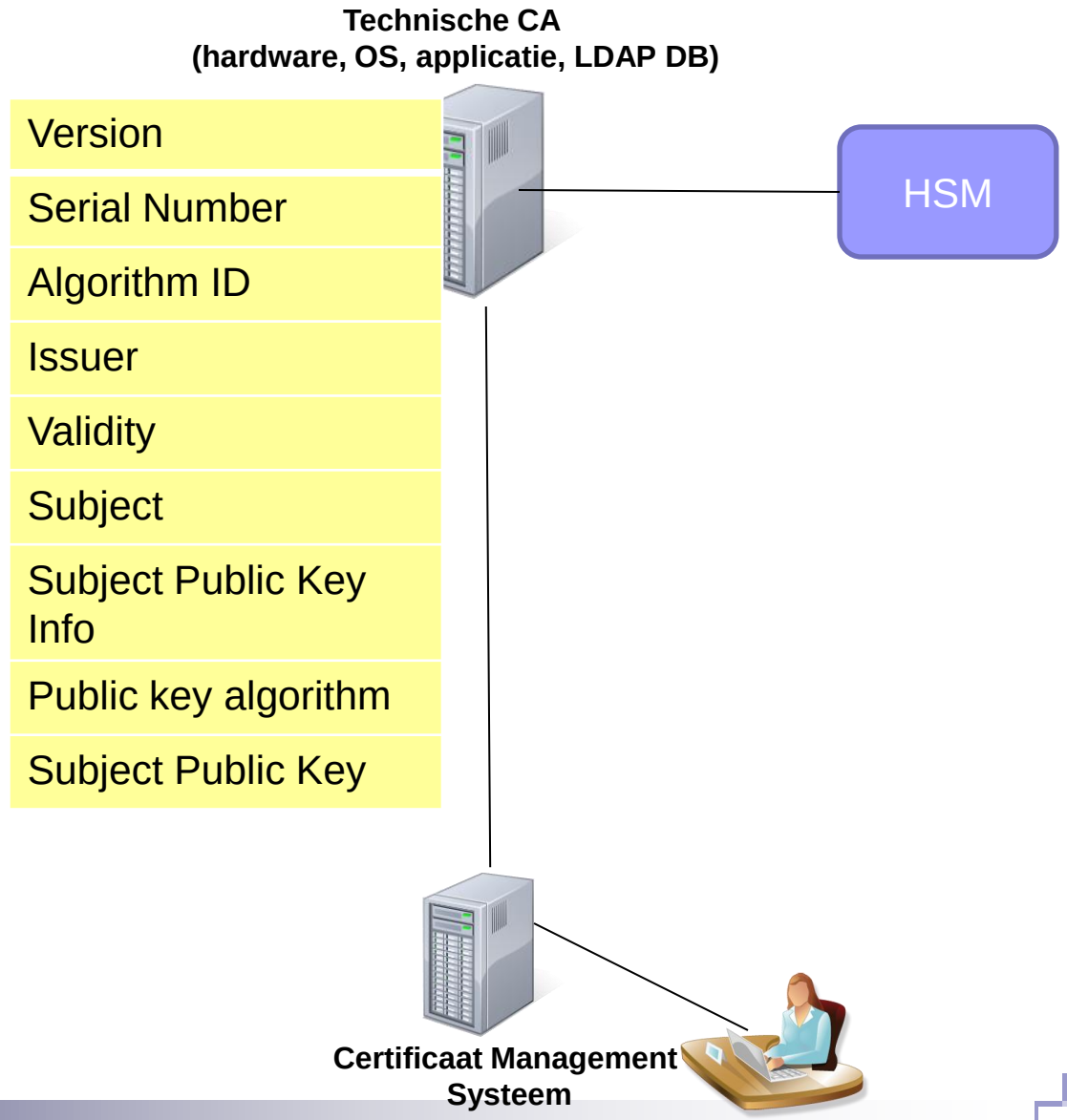
- Context
- Verbeter suggesties HSM opzet binnen CSPs (langere termijn)
- Verbeter suggesties HSM opzet binnen CSPs (kortere termijn)
- Verbeterde technische monitoring via nieuw type HSM
- Afsluiting

Reguliere technische opzet CSP



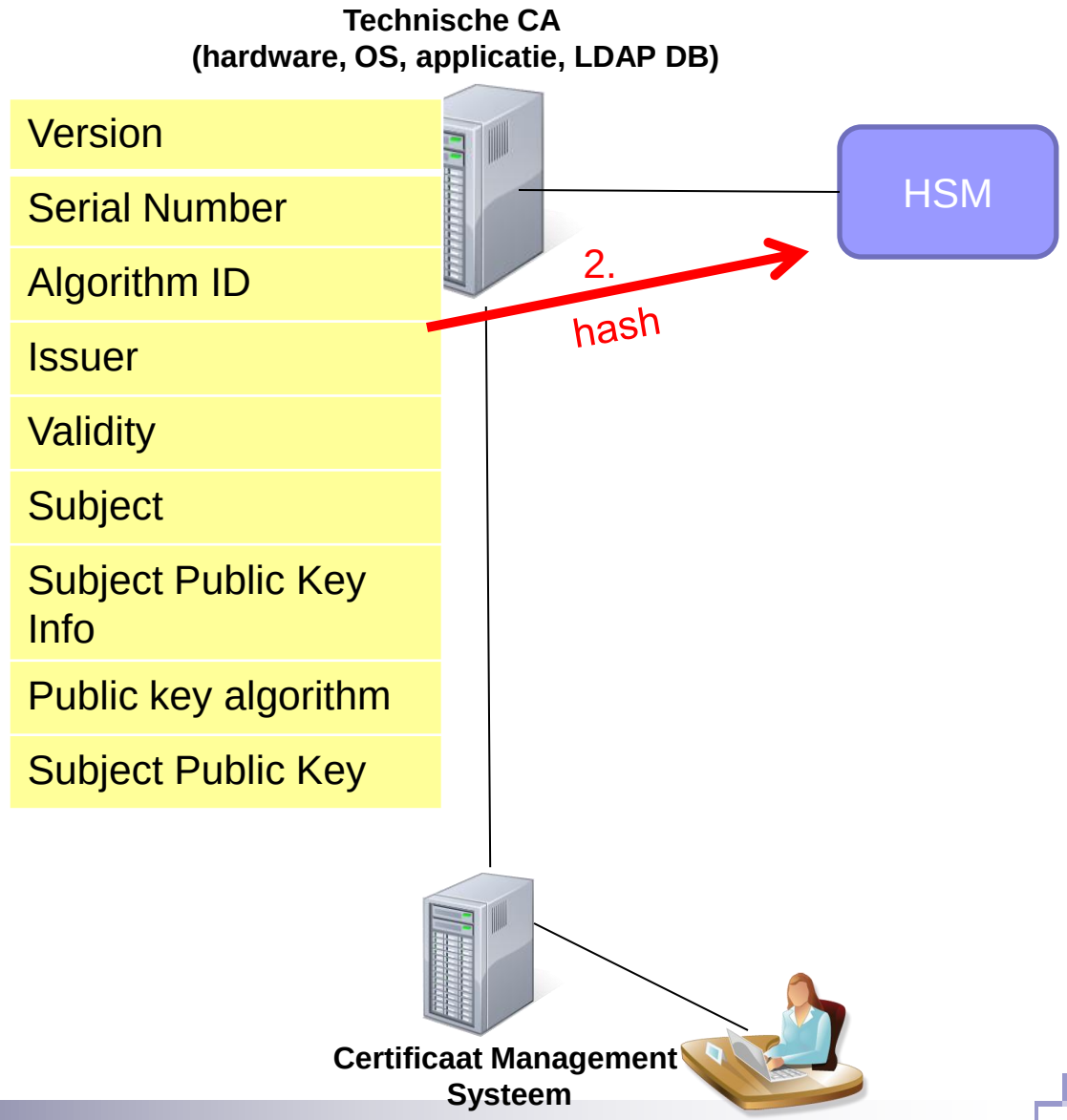
Reguliere technische opzet CSP

1. CMS/CA genereert alle certificaat velden



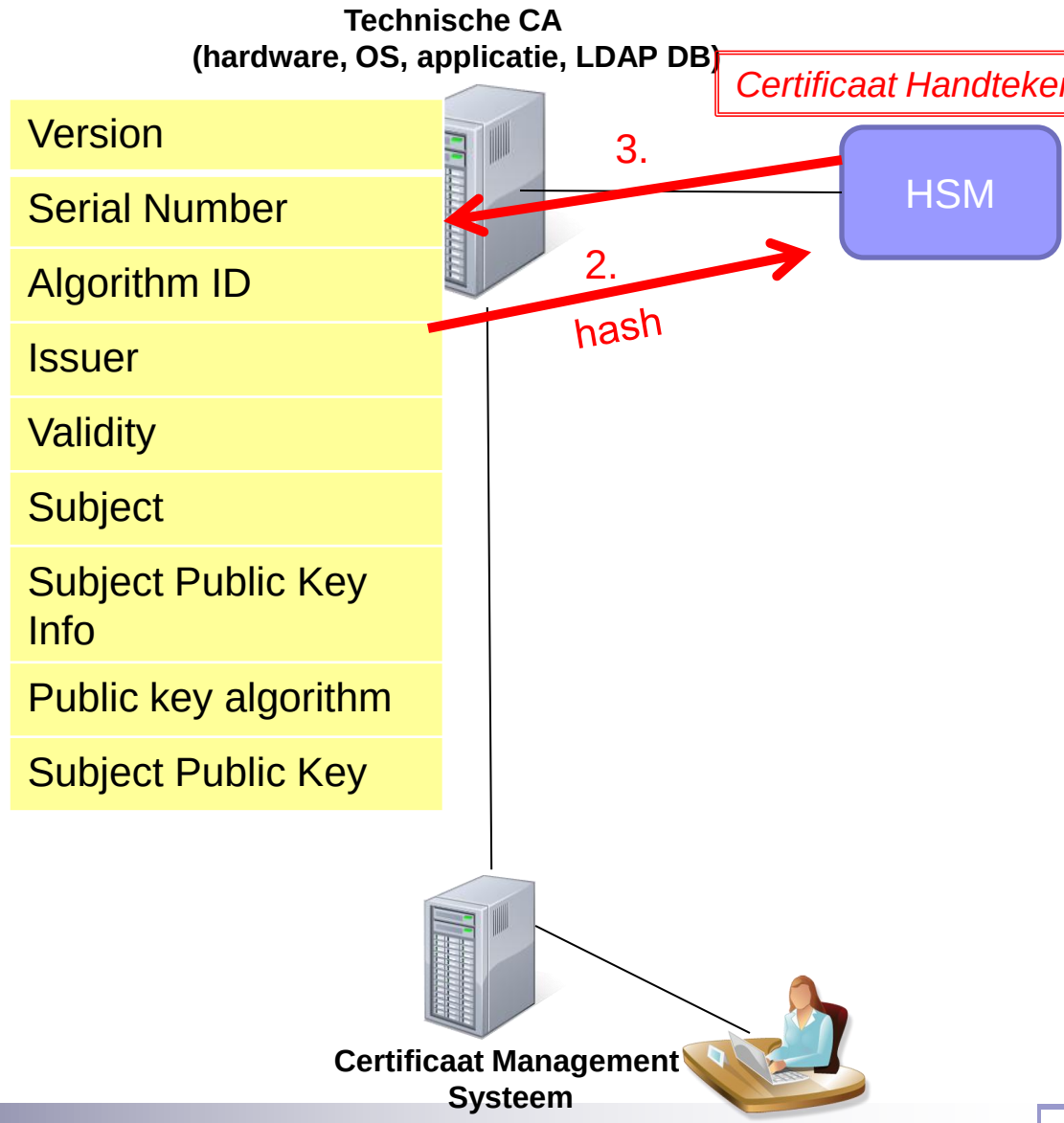
Reguliere technische opzet CSP

1. CMS/CA genereert alle certificaat velden
2. CA berekent hash en stuurt deze naar HSM over veilig kanaal



Reguliere technische opzet CSP

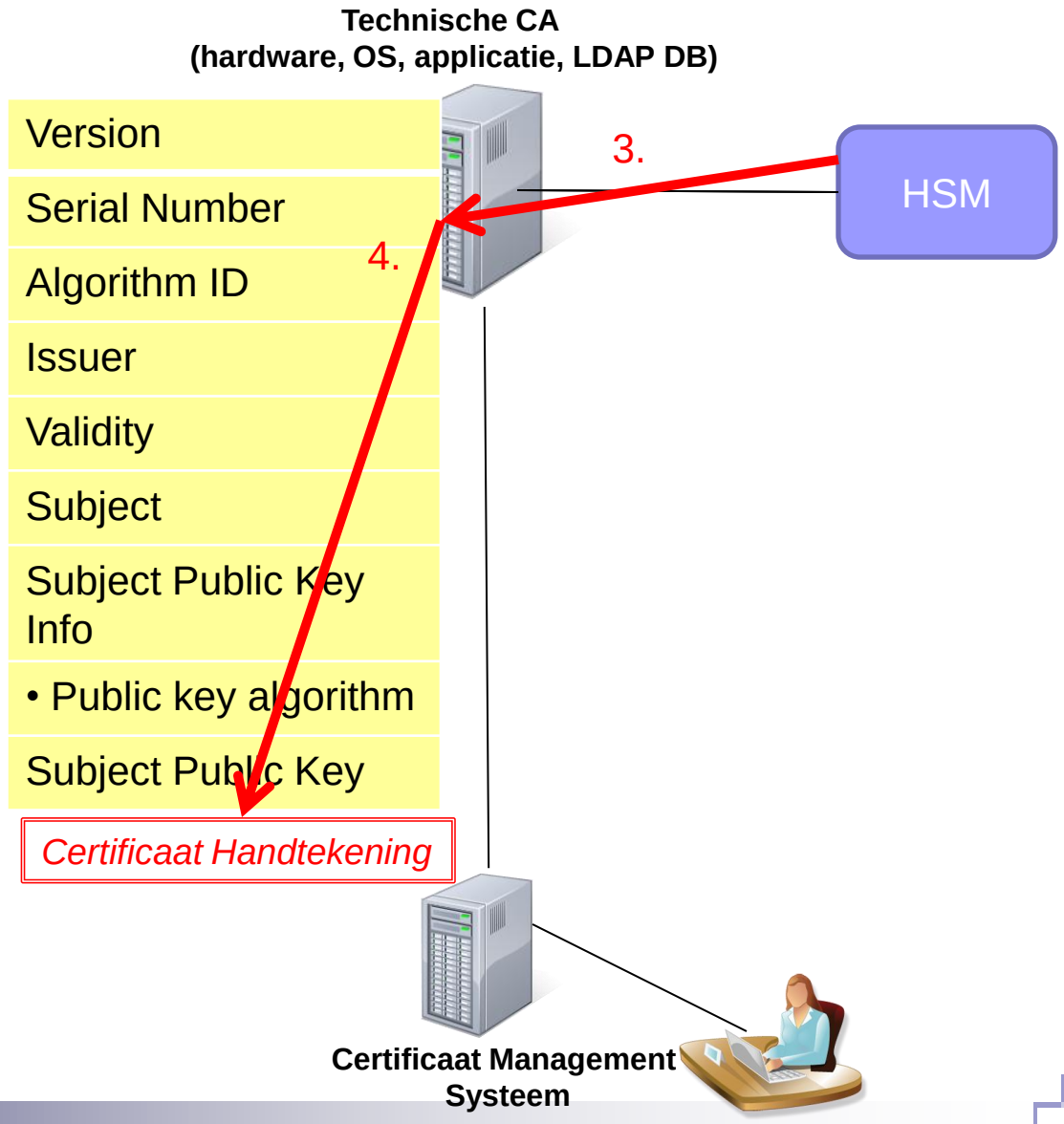
1. CMS/CA genereert alle certificaat velden
2. CA berekent hash en stuurt deze naar HSM over veilig kanaal
3. HSM genereert certificaat handtekening en stuurt dit naar CA.



Reguliere technische opzet CSP

1. CMS/CA genereert alle certificaat velden
2. CA berekent hash en stuurt deze naar HSM over veilig kanaal
3. HSM genereert certificaat handtekening en stuurt dit naar CA.
4. CA ontvangt handtekening en vormt certificaat (vormt logs, voegt toe aan LDAP)

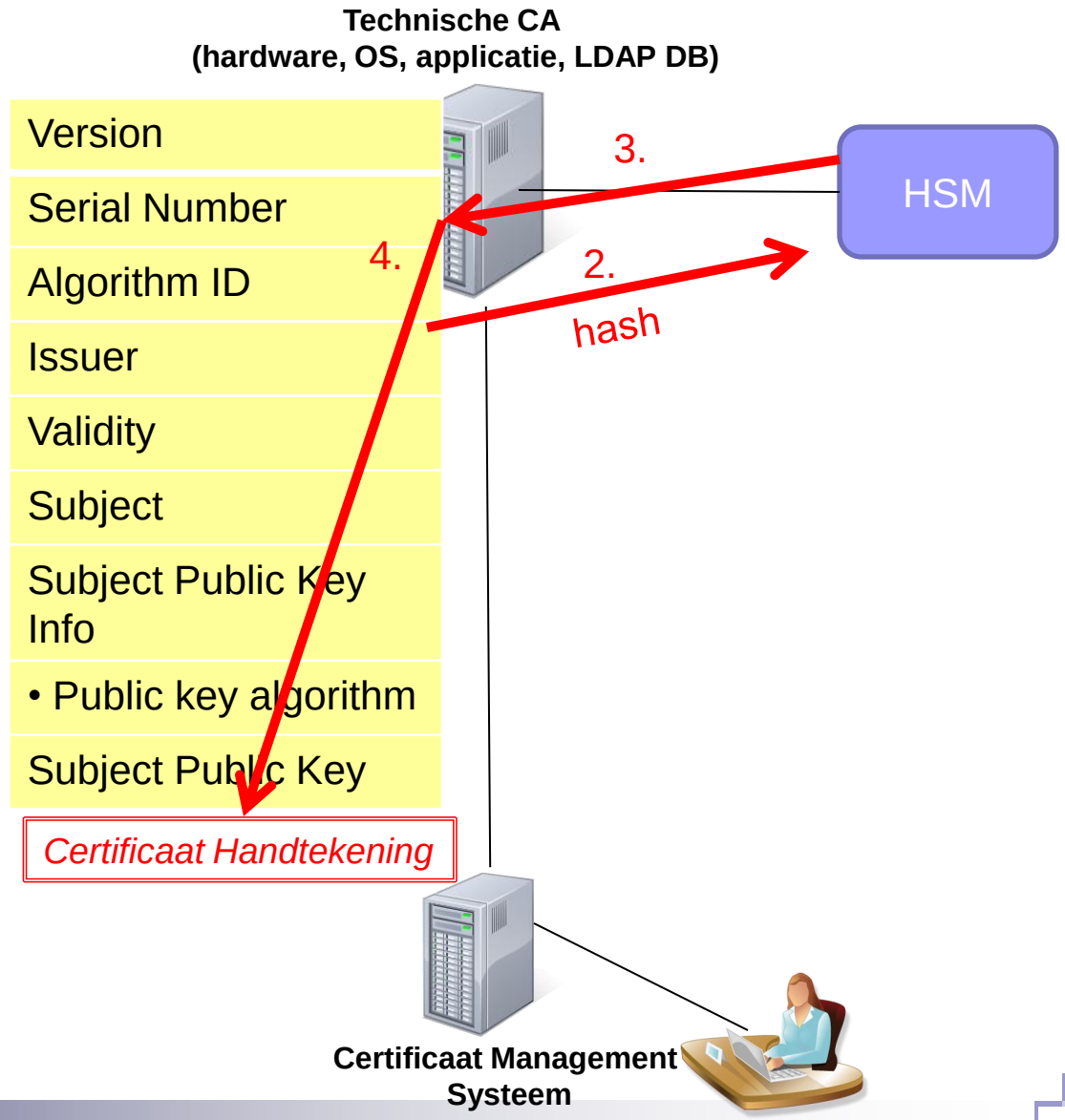
Noot: HSM gedraagt zich als een smartcard, zonder besef van wat hij tekent.



Gecompromiteerde CA

A. Als de CA en diens logs en LDAP database gecompromiteerd raken dan kan de CSP niet meer vaststellen wat er is geproduceerd.
B. Specifiek weet de CSP niet welke certificaat serienummers illegaal zijn uitgegeven; en dus ook niet welke serienummers op de Certificate Revocation List (CRL) moeten.

- *CA compromitering is grote calamiteit, niet weten wat geproduceerd is, kan fatale calamiteit zijn.*

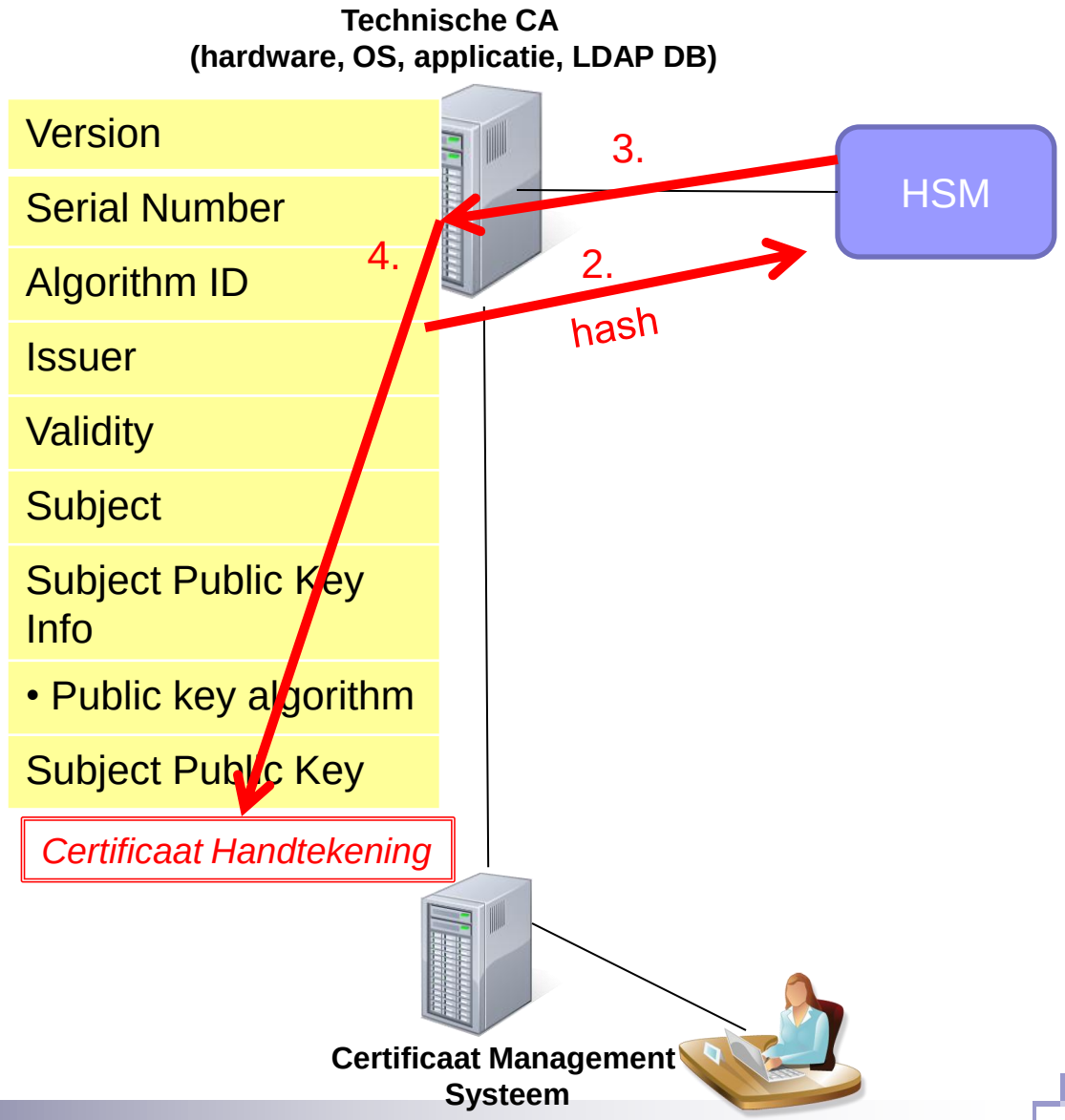


Gecompromiteerde CA: mitigatie

- *Als* de aanvaller de standaard routines van de CA gebruikt *en* de serienummers zijn reproduceerbaar (*) dan kan de CSP voorspellen welke serienummers ontbreken en op de CRL moeten worden gezet.

(*)

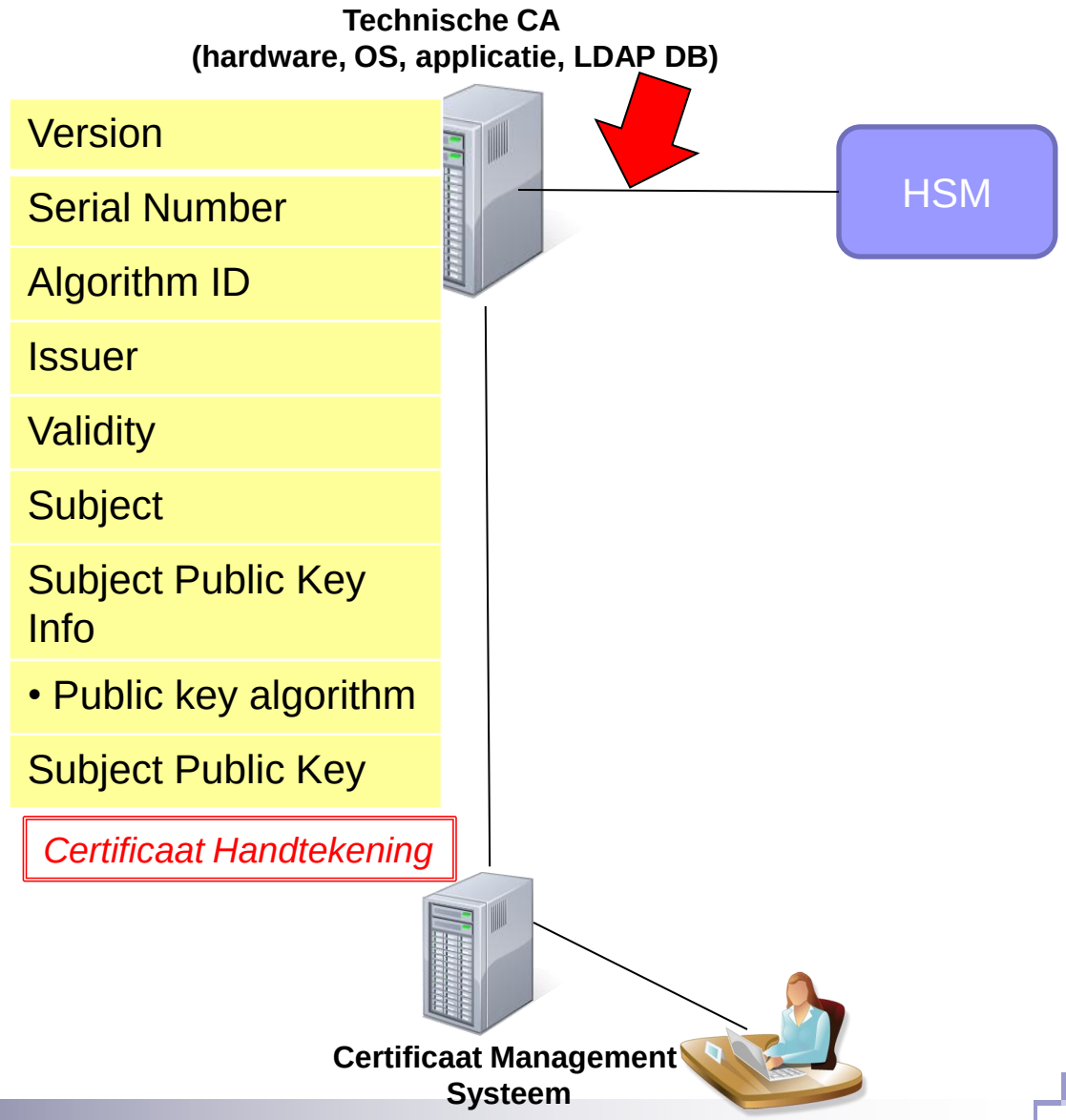
- CSPs moeten minimaal weten hoe de serienummers worden gegeneerd door hun technische CA.
- Opvolgende serienummers kunnen voorzien in reproduceerbaarheid, maar hebben mogelijk commerciële nadelen.



Gecompromiteerde CA: mitigatie

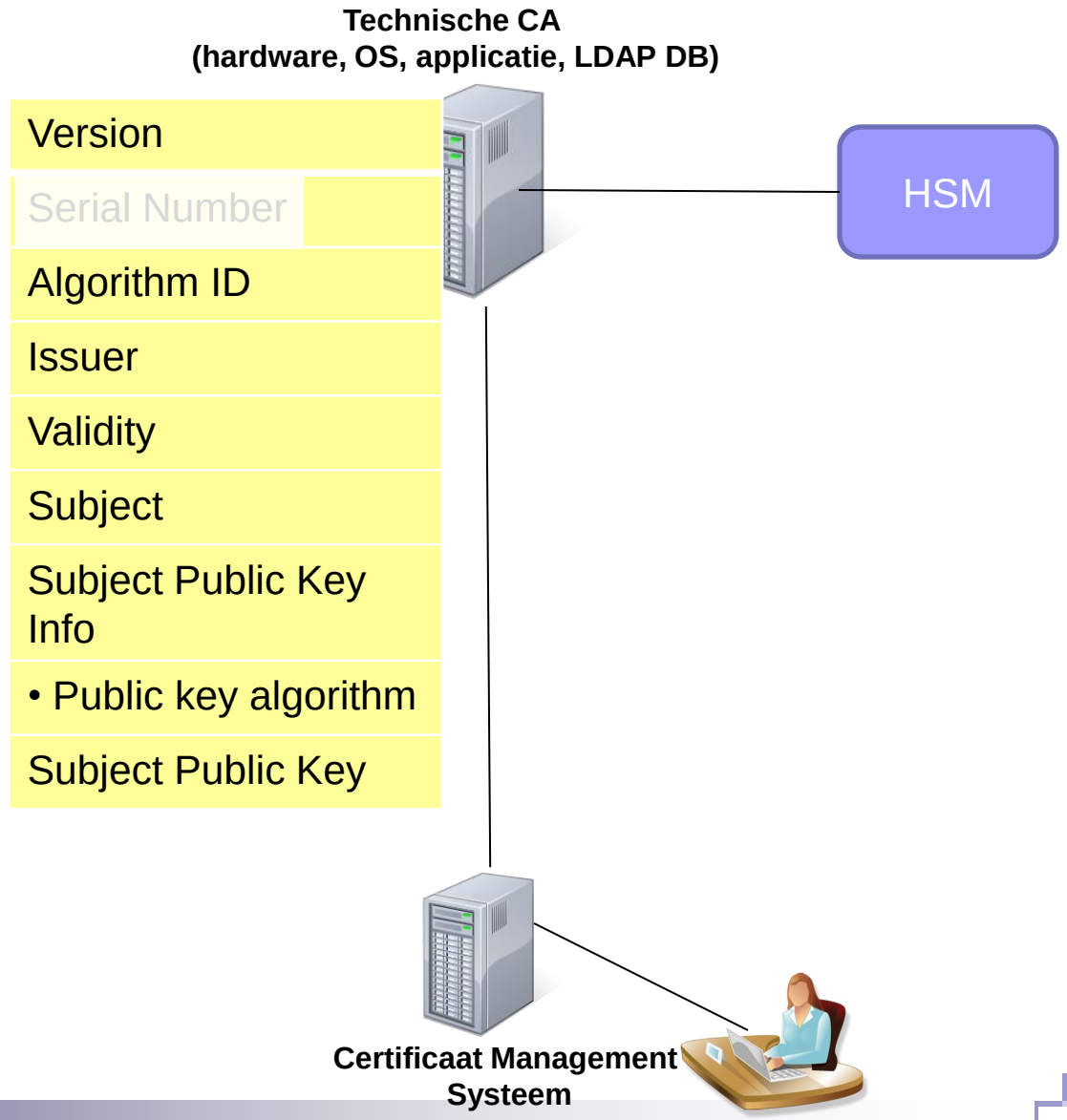
- Omdat de CA gebaseerd is op software is het moeilijk zekerheid te hebben dat de aanvaller inderdaad de standaard routines van de CA heeft gebruikt.
- De aanvaller kan ook de connectie tussen de CA en HSM hebben ‘ge-hijacked’ en zo zijn eigen serienummers hebben gemaakt.
- De aanvaller kan ook een eventuele connectie met een syslog server of WORM archief (DVD) verbreken.

- HSM is de natuurlijke plaats om zekerheid over serienummers te krijgen.



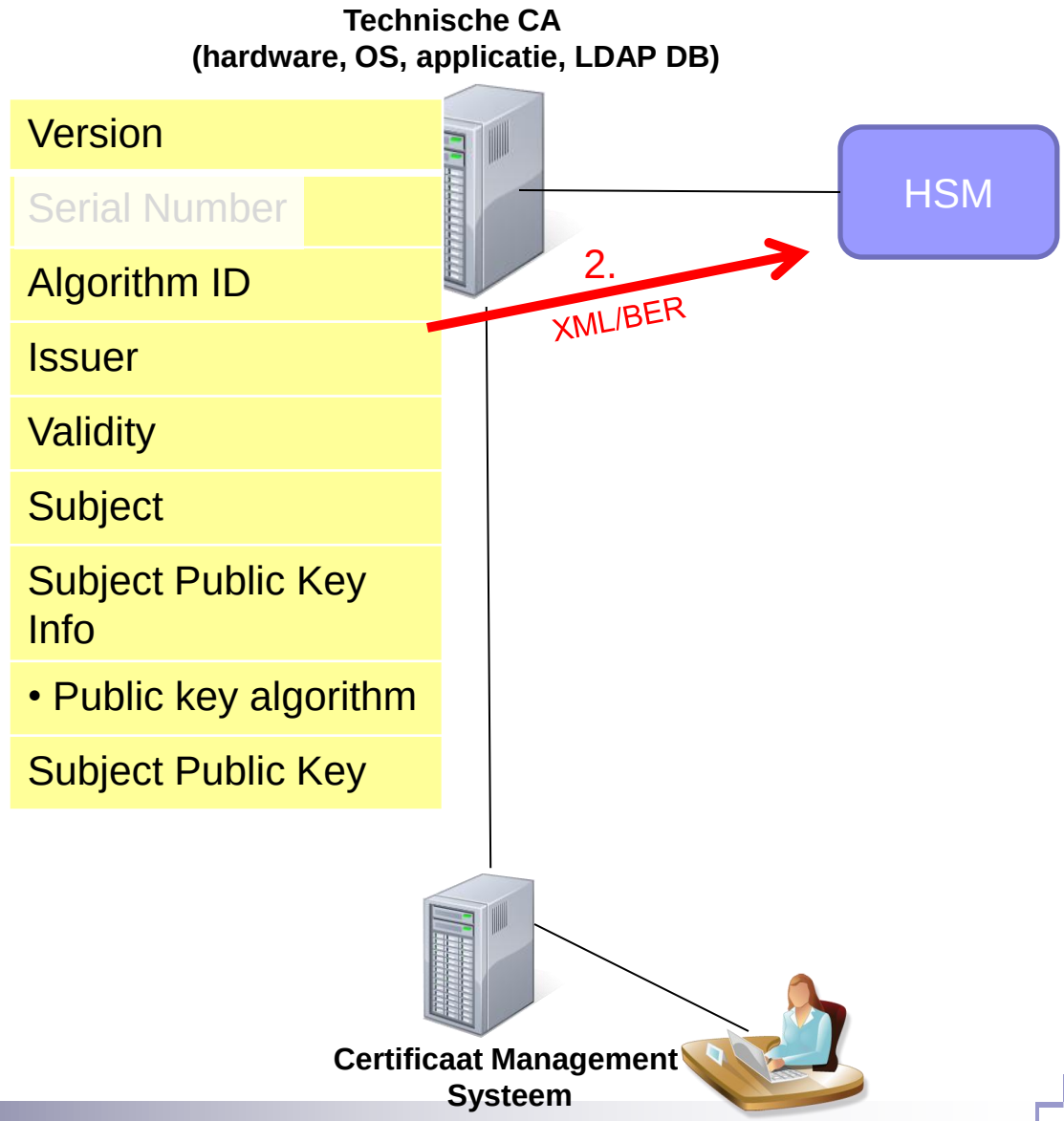
Mogelijk nieuw type HSM

1. CMS/CA genereert alle certificaat velden maar niet het serienummer.



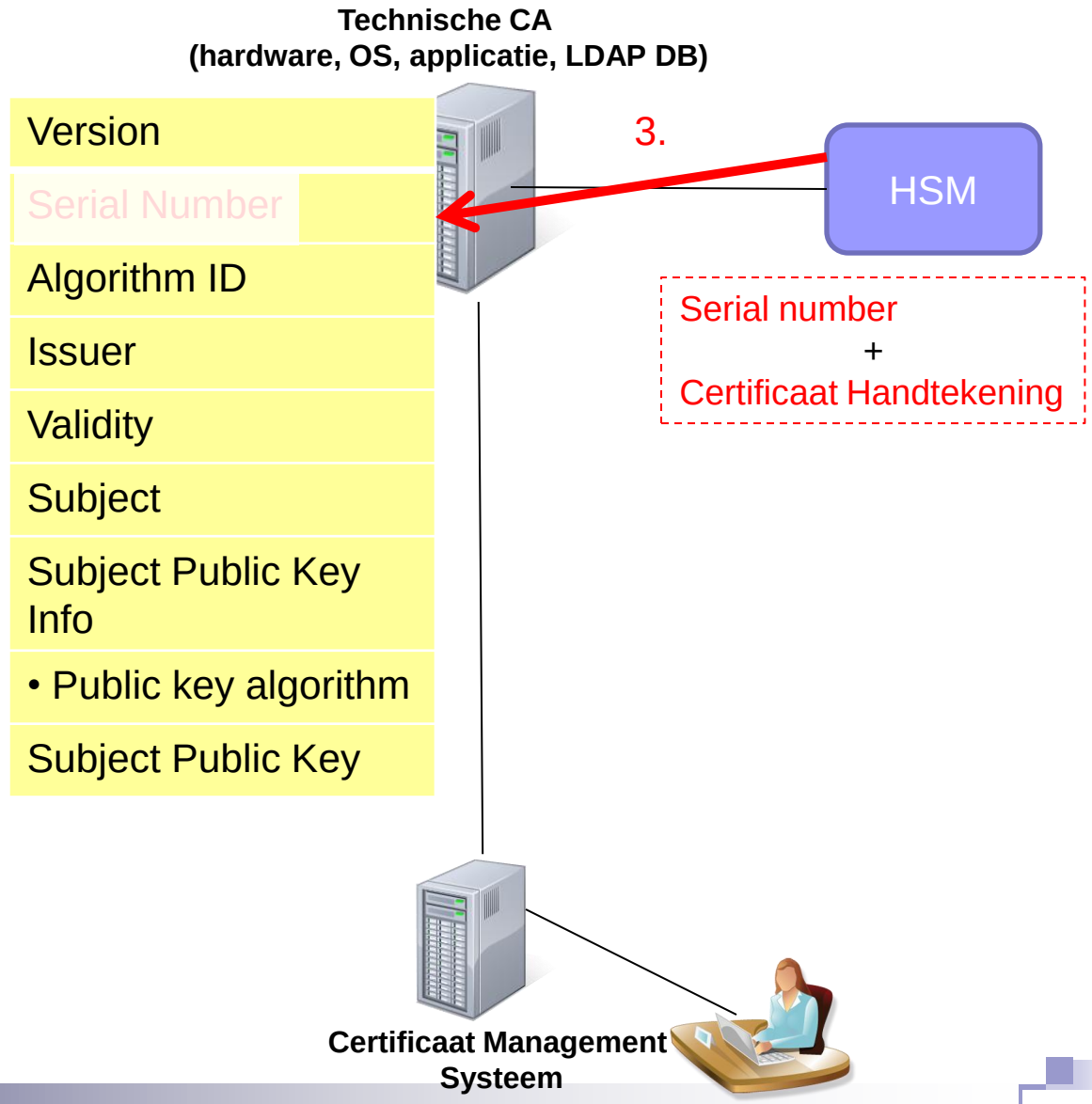
Mogelijk nieuw type HSM

1. CMS/CA genereert alle certificaat velden maar niet het serienummer.
2. CA genereert certificaat velden en stuurt deze als bericht (XMLof BER) naar HSM over veilig kanaal.



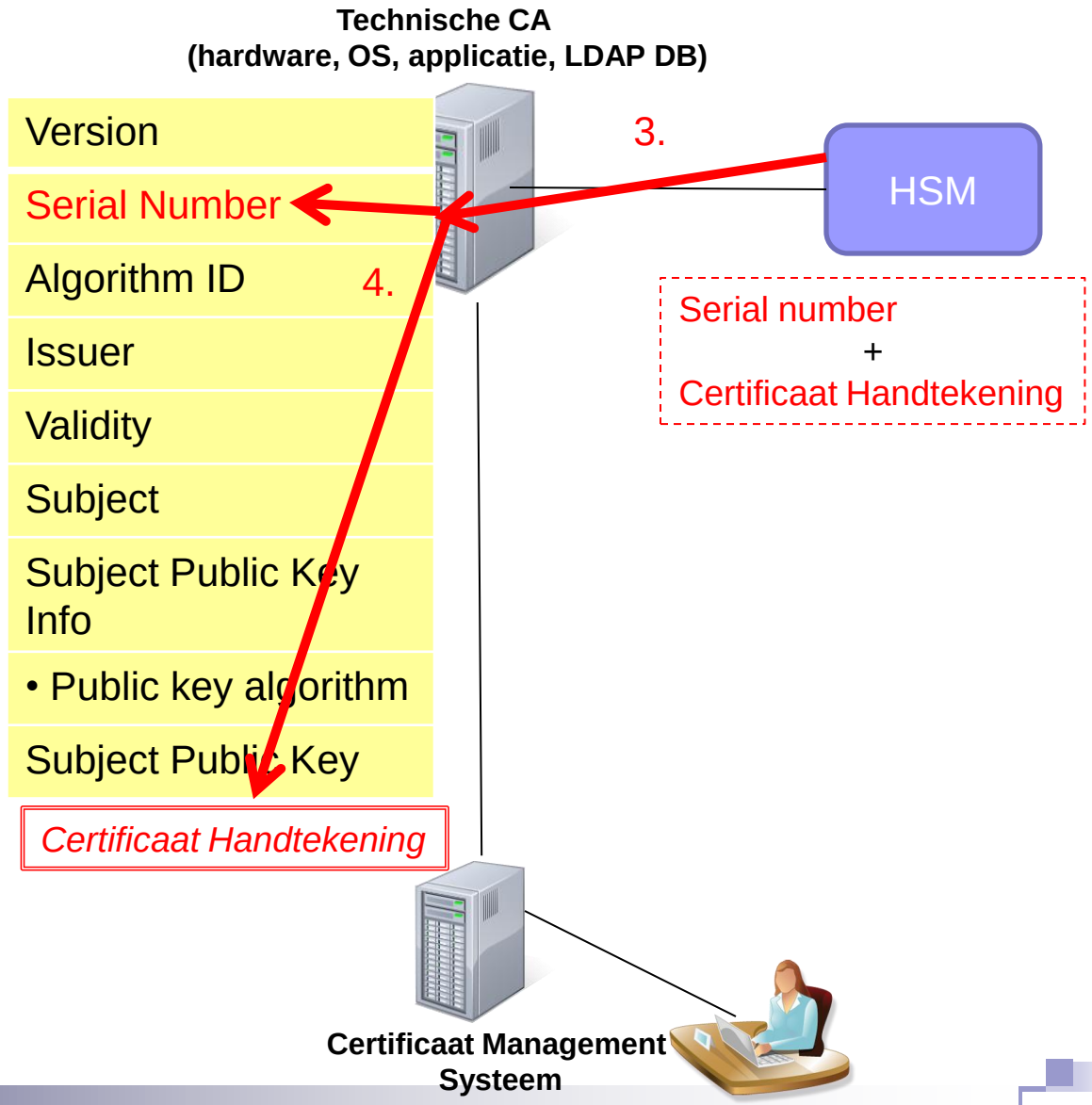
Mogelijk nieuw type HSM

1. CMS/CA genereert alle certificaat velden maar niet het serienummer.
2. CA genereert certificaat velden en stuurt deze als bericht (XMLof BER) naar HSM over veilig kanaal.
3. HSM genereert serienummer, berekent hash over de velden en daarover een certificaat handtekening; stuurt beide naar CA.



Mogelijk nieuw type HSM

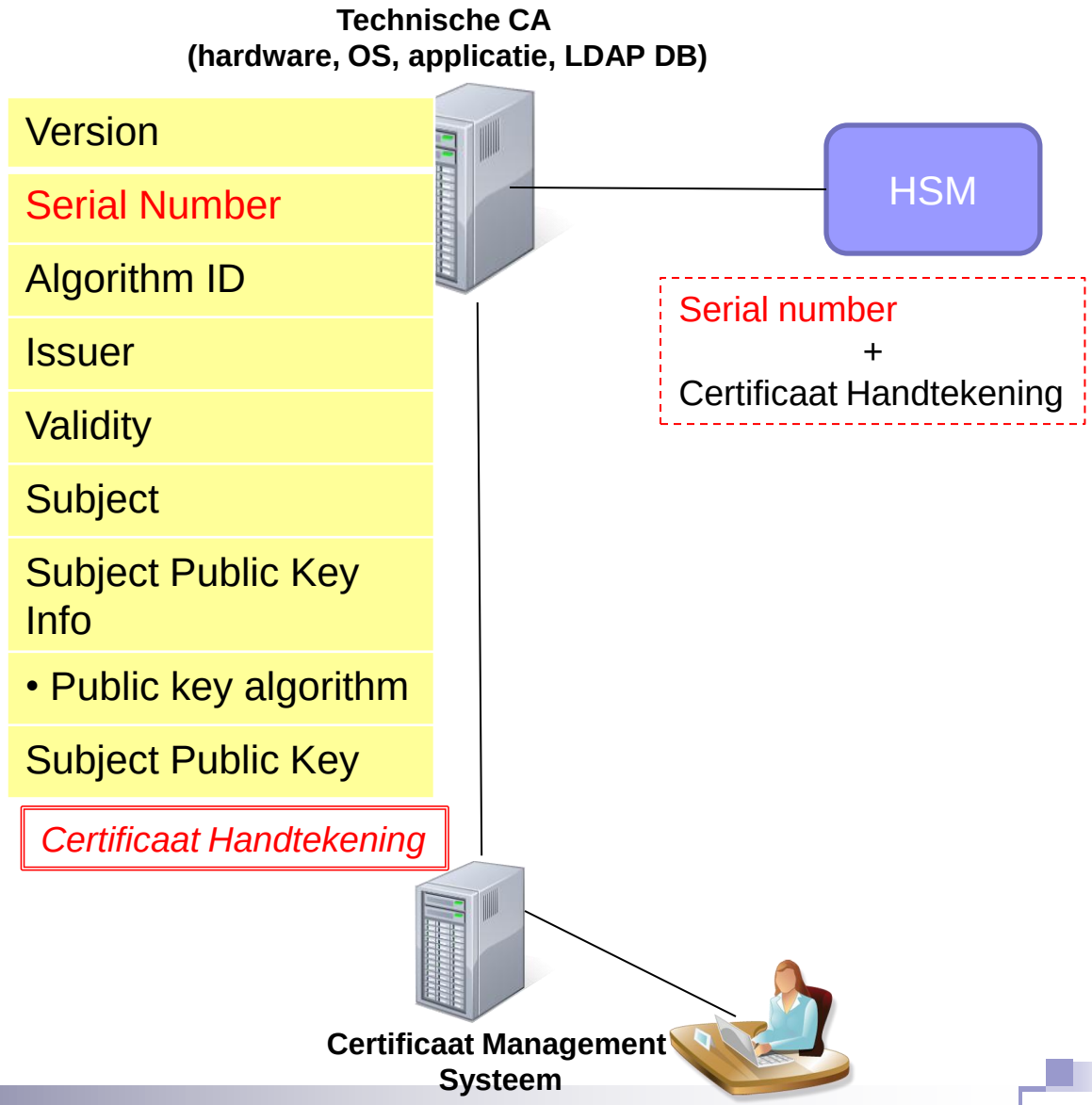
1. CMS/CA genereert alle certificaat velden maar niet het serienummer.
2. CA genereert certificaat velden en stuurt deze als bericht (XMLof BER) naar HSM over veilig kanaal.
3. HSM genereert serienummer, berekent hash over de velden en daarover een certificaat handtekening; stuurt beide naar CA.
4. CA vormt certificaat (plaatst serienummer en certificaat handtekening), valideert, maakt logs en voegt certificaat toe aan LDAP.



Mogelijk nieuw type HSM

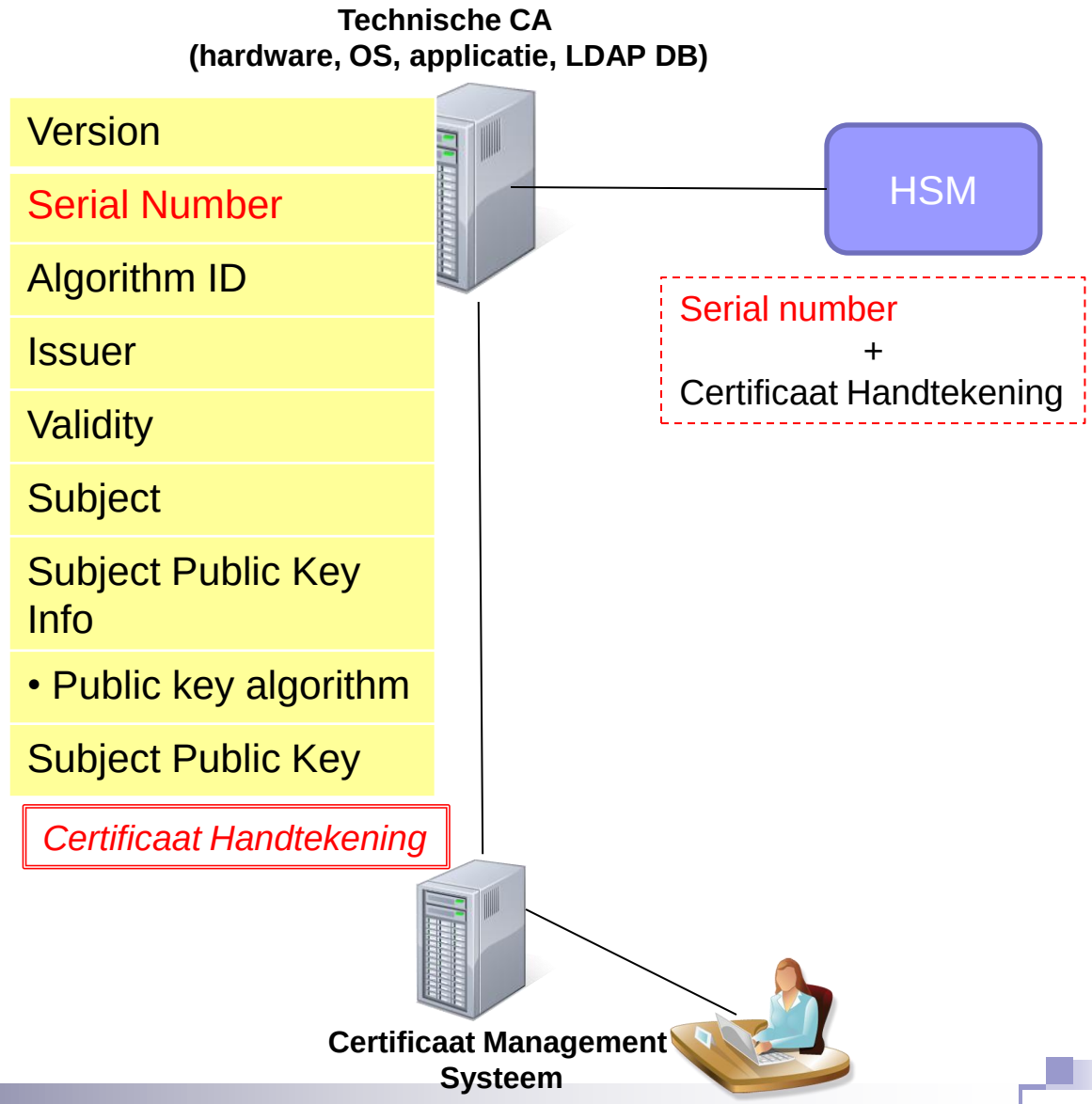
- De HSM houdt de serienummers bij en kan een lijst van de gegenereerde serienummers produceren in de juiste volgorde.(*)
- Een (gecompromiteerde) CSP kan via HSM vaststellen welke serienummers zijn geproduceerd na het laatste ‘valide’ certificaat en deze op de CRL zetten.

(*)
- De HSM kan versleutelde sequentie nummers gebruiken en laatste sequentie nummer als veilige HSM teller opslaan.
- Optioneel kan HSM ook anderecertificaat info loggen, m.n., Subject’ attribuut.



Mogelijk nieuw type HSM

- De HSM laat geen ander gebruik van de bewuste signing key toe zoals het tekenen van hashes.
- Om eventuele (fysieke) vernietiging van HSM door aanvaller te mitigeren, moet het serienummer generatie algoritme bij voorkeur ook buiten de CSP worden opgeslagen (‘sleutel’).
- Daarbij kan er een beperking komen op het aantal serienummers dat kan worden geproduceerd; e.g., na 100 certificaat serienummers moet de HSM weer worden vrijgegeven.

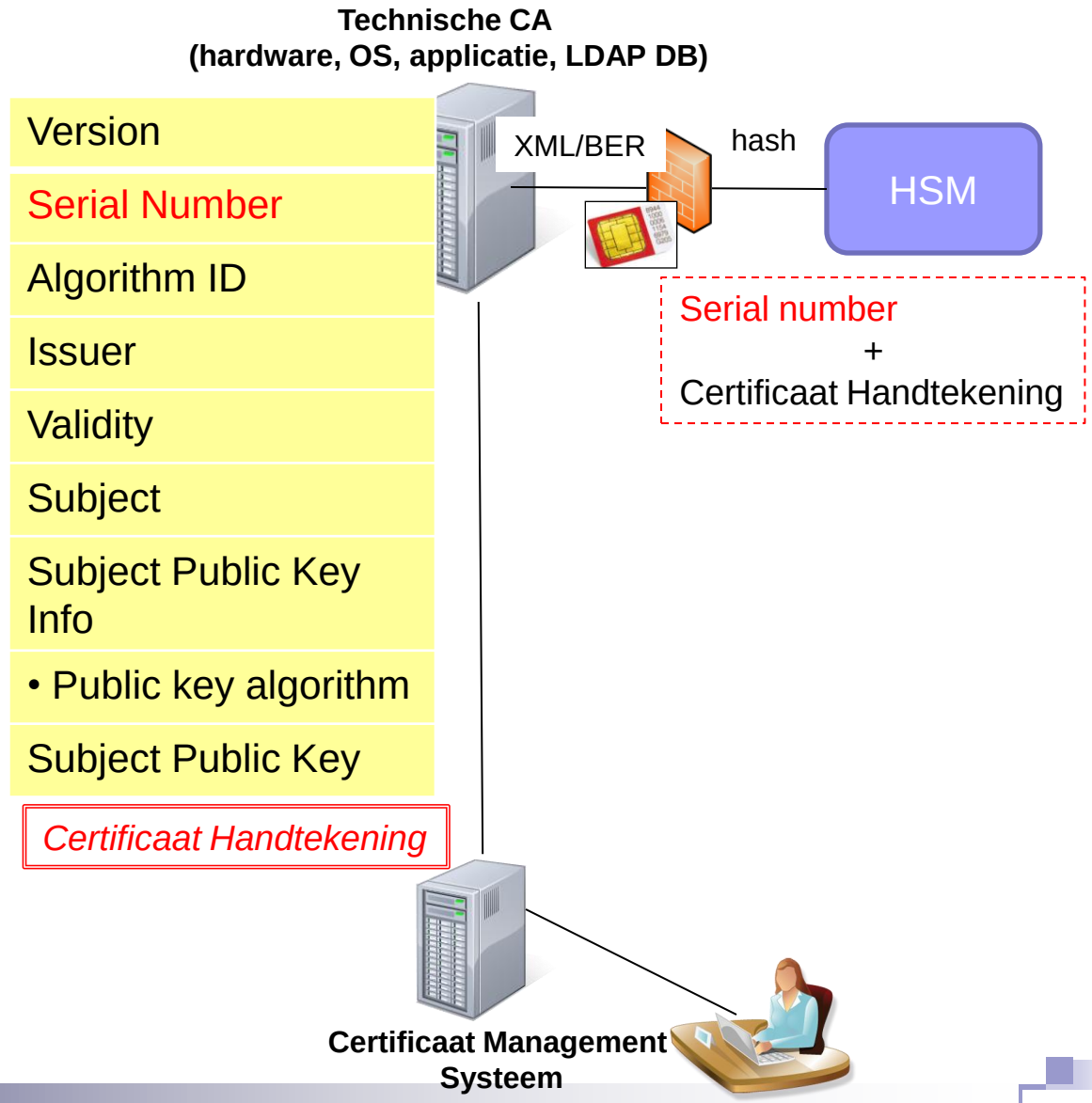


Agenda

- Context
- Verbeter suggesties HSM opzet binnen CSPs (langere termijn)
- Verbeter suggesties HSM opzet binnen CSPs (kortere termijn)
- Verbeterde technische monitoring via nieuw type HSM
- Afsluiting

Mogelijk nieuw type HSM op kortere termijn

- Nieuw type HSM moet FIPS 140-2 level 3 gecertificeerd worden en dat is tijdrovend.
- Een snellere (‘*compliant*’) tussenoplossing is de plaatsing van dedicated device tussen CA en bestaande HSM: hardened en voorzien van Javacard applicatie.

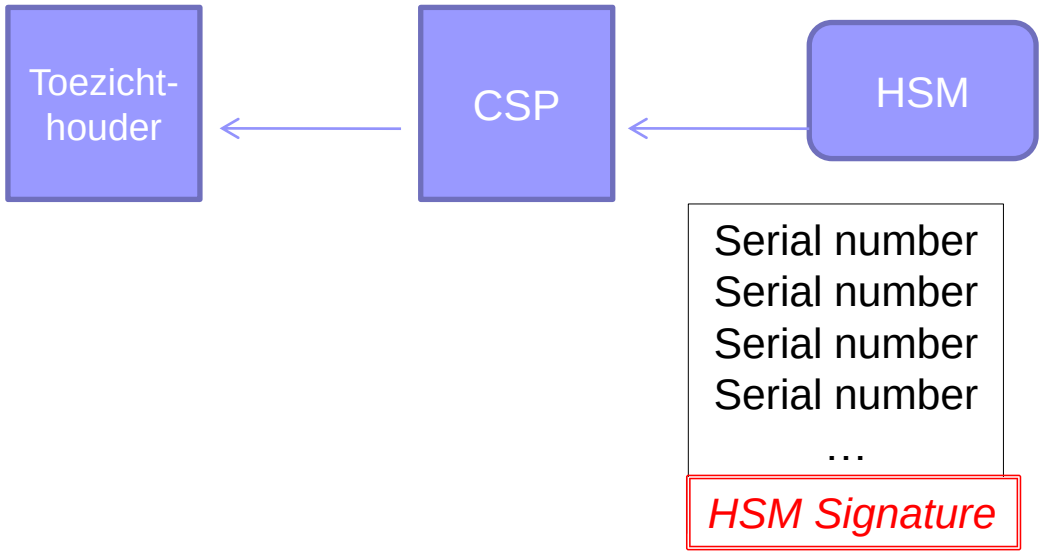


Agenda

- Context
- Verbeter suggesties HSM opzet binnen CSPs (langere termijn)
- Verbeter suggesties HSM opzet binnen CSPs (kortere termijn)
- Verbeterde technische monitoring via nieuw type HSM
- Afsluiting

Nieuw type technisch toezicht

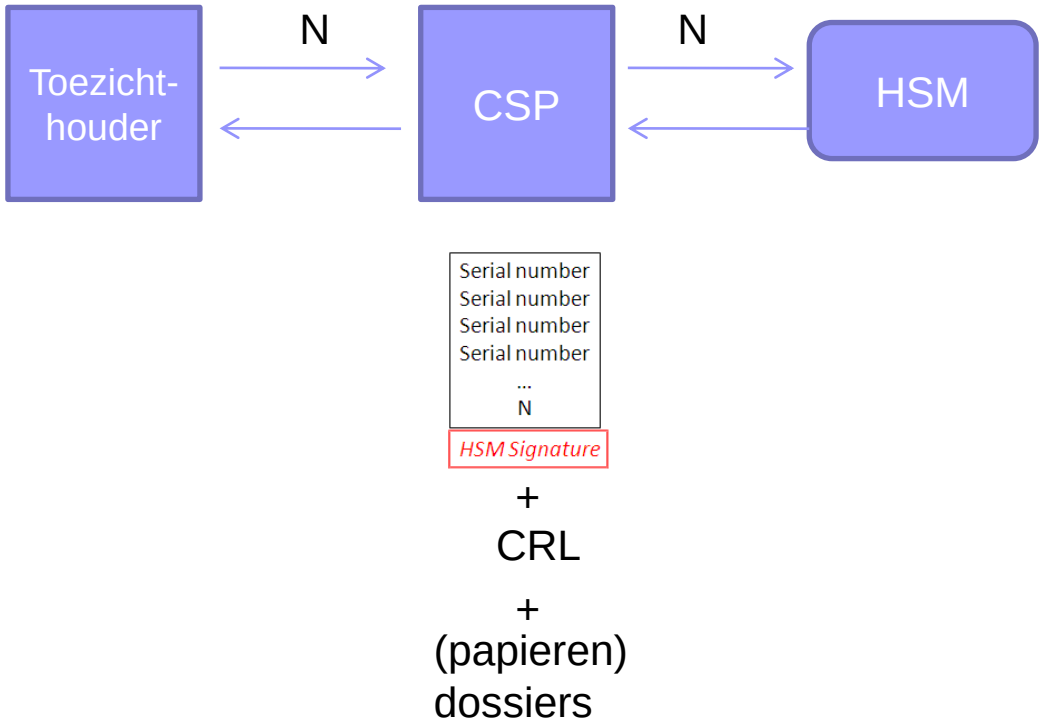
Setup: toezichthouder woont het sleutel generatie proces bij en ontvangt een HSM handtekening verificatie sleutel.



Technisch toezicht

Toezichthouder krijgt periodiek:

I. Actuele lijst met uitgegeven serienummers van CSP, getekend door HSM.
II. up-to-date CRL
III. Kopieën van (papieren) dossiers van legitieme certificaten inclusief revocatie logs (e.g., extract vanuit CMS).



(*) Om actualiteit zeker te stellen kan de toezichthouder een random getal N sturen dat deel moet uitmaken van de getekende lijst.

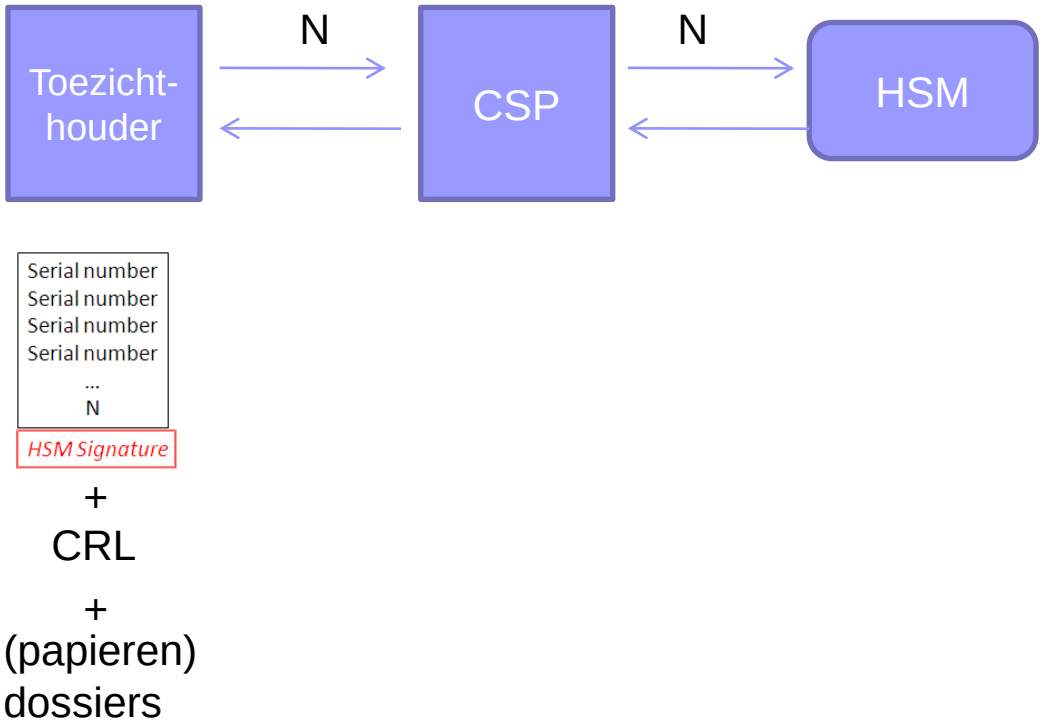
Technisch toezicht

Toezichthouder krijgt periodiek:

I. Actuele lijst met uitgegeven serienummers van CSP, getekend door HSM.
II. up-to-date CRL
III. Kopieën van (papieren) dossiers van legitieme certificaten inclusief revocatie logs (e.g., extract vanuit CMS).

→ Toezichthouder controleert consistentie :
  a) I = III, *of*
  b) I ≠III *maar* I= II ∪ III

- Bij b) moet de CSP nadere toelichting geven.
- Als aan a) *én* b) niet voldaan is, dan zijn er valse certificaten in omloop.



(*) Om actualiteit zeker te stellen kan de toezichthouder een random getal N sturen dat deel moet uitmaken van de getekende lijst.