Proces certificaatwissel

In de metadata zijn één of meer actuele certificaten per deelnemer opgenomen. De deelnemers en de beheerorganisatie hebben de mogelijkheid om uit voorzorg ook certificaten op te geven die gebruikt (kunnen) gaan worden bij het wisselen van een certificaat. Dit maakt het netwerk minder kwetsbaar wanneer een certificaat gewisseld moet worden.

Dit proces beschrijft hoe het wisselen van certificaten verloopt.

Om het proces van het wisselen van een certificaat succesvol te laten verlopen, is het van belang dat deelnemers meerdere certificaten per deelnemer kunnen verwerken.

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De technisch beheerder van de beheerorganisatie is er verantwoordelijk voor dat de procesbeschrijving actueel blijft.

Overzicht processtappen

Toelichting processtappen

1. Aanleveren nieuwe certificaat	
Input	Geplande certificaatwissel bij een deelnemer
Activiteit	1. De deelnemer informeert de beheerorganisatie tijdig over de geplande certificaatwissel. 2. De deelnemer levert het nieuwe metadatabestand aan bij de beheerorganisatie, voorafgaand aan moment waarop het huidige certificaat verloopt. In deze metadata is opgenomen: • de huidige public key die in gebruik is • de nieuwe public key die de deelnemer wil gaan gebruiken 1. De beheerorganisatie aggregeert en publiceert de nieuwe metadata volgens het Proces netwerkmetadata, en attendeert alle deelnemers op de certificaatwissel. 2. De deelnemers MOETEN de nieuwe versie van de metadata binnen het eerstvolgende gebruikelijke Onderhoudsvenster doorvoeren. 3. Na het onderhoudsvenster MAG de betreffende deelnemer het nieuwe certificaat gebruiken.
Output	Doorgevoerde metadata met oude en nieuwe certificaat
Wie?	• Beheerorganisatie, technisch beheerder • Deelnemers, technisch beheerders

2. Verwijderen oude certificaat	
Input	Doorgevoerde metadata met oude en nieuwe certificaat
Activiteit	1. Wanneer het nieuwe certificaat overal binnen het netwerk is geaccepteerd, kan het oude certificaat uit de metadata worden gehaald. De betreffende deelnemer levert nieuwe metadata aan met daarin alleen de public key van het nieuwe certificaat. 2. De beheerorganisatie aggregeert en publiceert de nieuwe metadata volgens het Proces netwerkmetadata, en attendeert alle deelnemers op de certificaatwissel.
Output	Doorgevoerde metadata met enkel het nieuwe certificaat
Wie?	• Beheerorganisatie, technisch beheerder • Deelnemers, technisch beheerders

Certificaatwissel kan ook voorkomen bij certificaten die niet in de metadata zijn opgenomen. Voor de werking van Single Sign On heeft iedere Herkenningsmakelaar een eigen fysieke cookieserver op gezamenlijk domein *.sso.eherkenning.nl. Dit gezamenlijke domein wordt beheerd door de beheerorganisatie.

De cookieservers verzenden geen berichten maar maken wel gebruik van certificaten. Wanneer deze certificaten worden gewisseld, wordt ongeveer hetzelfde proces doorlopen als bij de certificaatwissel in metadata. Dat proces verloopt dan als volgt:

- De deelnemer meldt tijdig (minimaal twee weken van te voren) bij de beheerorganisatie dat het certificaat moet worden gewisseld via de issuetracker Mantis. Hierbij vermeldt de deelnemer de huidige public key die in gebruik is, de nieuwe public key en de termijn waarop de wijziging moet plaatsvinden.
- De beheerorganisatie vervangt de public key van de betreffende deelnemer.
- De deelnemer ontvangt een bevestiging van de beheerorganisatie via Mantis wanneer de vervanging is afgerond.
- De deelnemer KAN nu het nieuwe certificaat gebruiken.