Memo

Aan:
Datum: 20170121
Van: Kennisnet
Onderwerp: Voorstel toepsassen DUO ODOC certificaat naast PKI Overheid als 'SAAS certificaat'

Voorstel:
In OSO'16 is het 'SAAS model' ingevoerd, waarbij leveranciers een PKI Overheidscertificaat gebruiken om in de OSO keten geïdentificeerd te worden. Een PKI overheidscertificaat bevat oa het organisatie identificerende nummer (OIN) waarmee een leverancier in de keten door het TC gecontroleerd kan worden.

DUO geeft ook certificaten uit, de zogenaamde ODOC certificaten. Oorspronkelijk bedoelt voor gebruik als 'schoolcertificaat', zijn deze nu ook beschikbaar voor leveranciers en worden als zodanig toegepast (bijvoorbeeld de MBO keten).

Het voorstel is om deze DUO ODOC certificaten naast PKI Overheidscertficaten al SAAS certificaat toe te gaan passen binnen OSO. Partijen kunnen dan kiezen of ze een PKI Overheid of DUO ODOC certificaat toepassen in de keten.

Voordelen van het toevoegen van DUO ODOC certificaten zijn:
- Partijen die al een DUO ODOC certificaat hebben, hoeven geen nieuw certificaat te kopen
- Toepassen van DUO ODOC brengt OSO in lijn met Edukoppeling.

Wijzigingen en impact

Zowel het TC als systemen die optreden als bronsysteem, moeten het DUO ODOC certificaat valideren. Het technische formaat van het ODOC certificaat is vergelijkbaar met die van PKI Overheid, waardoor de impact in eerste instantie beperkt blijft. Echter op twee plaatsen zijn aanpassingen nodig:

Controleren van client
Als een systeem bevraagd wordt (opvragen dossier, TC) door een ander systeem, moet vastgesteld worden dat het certificaat van de bevragende partij correct is. Hiervoor moet de complete keten van uitgifte worden afgelopen. Deze certificaatketen wijkt in ODOC af van die van PKI Overheid. Het controleren van de certificaatketen zal uitgebreid moeten worden met een tweede geaccepteerde keten die afgelopen moet worden. De correcte implementatie hiervan zal bij de kwalificatietesten worden meegenomen; afgelopen jaar bleek dit een 'pittig' onderdeel(!). De impact hiervan schat ik daarom in om aanzienlijk.

Controleren van server
Het PKI ODOC certificaat kan ook toegepast worden als middel om het bevraagde systeem, de server, te controleren. Een client zal alleen een verbinding opzetten als de server een 'vertrouwd' (trusted) partij is.

Om dit voor een PKI certificaat te implementeren, moet het PKI certificaat van de server in de trust store van de client worden opgenomen. Voor PKI overheid is dit automatisch het geval, omdat PKI overheid is opgenomen in een wereldwijde 'trust' van partijen. Voor PKI ODOC is dit niet het geval en moet de 'root' van ODOC in de trust store worden opgenomen. Dit is dus (mits op root niveau) een eenmalige actie voor iedere leverancier, met een beperkte impact.