edustandaard

Onderwerp: **Analyse toepassing ODOC certificaten**
Van: **Edustandaard**
Voor: **Werkgroep Edukoppeling**
Datum: **20-3-2017**
Status: **Concept**

Aanleiding

Het toepassen van ODOC certificaten, voor zowel scholen als voor SaaS-leveranciers, is al sinds Edukoppeling versie 1.1 toegestaan en er is altijd verondersteld dat partijen hier vrij eenvoudig mee konden werken. Recent is bij het OSO Technisch Overleg naar voren gekomen dat partijen het toch als een barrière ervaren om ODOC certificaten toe te staan naast PKIoverheid certificaten. Het levert extra werk op in de keten. Bovendien vragen de leveranciers zich af hoe toekomstbestendig ODOC is en of inspanningen die ervoor nodig zijn maar tijdelijk benut kunnen worden. Het OSO Technisch Overleg heeft dan ook besloten dat alleen PKIoverheid certificaat gebruikt mogen worden.

Deze situatie werd besproken tijdens de Edukoppeling werkgroep van 8 februari 2017. De conclusie was dat het in principe onwenselijk is dat er per keten hier verschillend mee omgegaan wordt. Het idee achter Edukoppeling is juist dat als deze logistieke koppeling eenmaal voor een keten is ingericht deze hergebruikt kan worden. Er is dan ook besloten dat het toepassen van ODOC certificaten nader onderzocht moet worden. Daartoe is deze notitie opgesteld. Deze kan gebruikt worden voor besluitvorming hoe we hier ten aanzien van de Edukoppeling standaard mee om willen gaan (actiepunt #0058).

Context

Er zijn verschillende scenario's te onderkennen die voor deze notitie relevant zijn. Het gaat hierbij om het volgende:

1. De onderwijsinstelling neemt als eindorganisatie een dienst af van een SaaS-leverancier. De SaaS-leverancier als logistieke dienstverlener beheert de betreffende koppelingen die met deze dienst samenhangen en communiceert met externe partijen onder de identiteit van de onderwijsinstelling en met diens certificaat. De logistieke header bevat de identiteit van de eindorganisatie, de onderwijsinstelling.
2. De onderwijsinstelling heeft als logistieke dienstverlener systemen en betreffende koppelingen in eigen beheer en communiceert onder eigen identiteit en met eigen certificaat.
3. De onderwijsinstelling neemt als eindorganisatie een dienst af van een SaaS-leverancier. De SaaS-leverancier als logistieke dienstverlener beheert de betreffende koppelingen die met deze dienst samenhangen en communiceert met externe partijen onder eigen identiteit met eigen certificaat. De logistieke header bevat de identiteit van de eindorganisatie.

Op zich hebben deze scenario's geen invloed op het toepassen van Edukoppeling, het eerste scenario wordt nu niet expliciet door de Edukoppeling standaard en de architectuur uitgesloten, maar wordt wel beschouwd als een verouderd en ongewenst scenario. Een onderwijsinstelling had in meerdere ketens verschillende certificaten nodig wat voor problemen en veel extra werk zorgde. Het werken met maar één certificaat in dit scenario zou veel voordeel opleveren. Omdat het nog steeds veel scholen betrof die dat ene certificaat nodig zouden hebben heeft DUO destijds besloten om als extra dienst ODOC certificaten te gaan leveren, waarbij het uitgifteproces voor scholen minder omslachtig kon worden ingericht en toch aan de benodigde eisen van identificatie kan worden voldaan gelijkwaardig aan die van PKIoverheid.
Het tweede en derde scenario beschrijven de gewenste situatie met een duidelijke scheiding van rollen conform Edukoppeling architectuur.

Probleemstelling

DUO levert binnen de onderwijssector ODOC certificaten aan marktpartijen en onderwijsinstellingen. Hiermee wordt de oplossing voor het probleem van vele certificaten in het eerste scenario ook gebruikt bij de toepassing van de Edukoppeling architectuur in het tweede en derde scenario. In principe is dit geen probleem, maar recent is in de OSO keten afgesproken dat ODOC certificaten worden uitgesloten omdat het toepassen van ODOC certificaten eerder extra effort/kosten met zich meebrengt dan dat dit voordelen oplevert. Het is niet wenselijk dat er in een bepaalde keten een ander (verplicht) logistiek koppelvlak ontstaat dan dat de Edukoppeling architectuur nu voorschrijft, dit ondermijnt het doel, het standaardiseren van een logistiek koppelvlak.

Omdat OSO nu formeel nog geen Edukoppeling voorschrijft en er nog een beperkt aantal ketens zijn die wel Edukoppeling 1.2 toepassen, is dit nu nog geen probleem. Voordat er meer implementaties komen moet hierin echter wel een duidelijk standpunt genomen worden. Kunnen ODOC certificaten bij een Edukoppeling koppelvlak gebruikt worden of te wel moeten we het voorschrift met de mogelijkheid om ODOC certificaten te gebruiken handhaven? Om deze vraag te kunnen beantwoorden worden een aantal relevante aspecten toegelicht, dit zijn:

1. Aansluiting op Digikoppeling
2. PKI certificaten
3. Toekomstvastheid ODOC certificaten
4. Ontwikkelingen bij PKIoverheid
5. Ontwikkelingen in andere domeinen

Aansluiting op Digikoppeling

Edukoppeling is afgeleid van Digikoppeling waar enkel PKIoverheid certificaten worden toegepast. In essentie zou dit ook voor Edukoppeling kunnen gelden als een onderwijsinstelling zelf de rol van logistieke dienstverlener uitvoert (tweede scenario) en onder de identiteit van bevoegd gezag kan communiceren. Er is dan geen behoefte aan een ODOC certificaat met een BRIN4 identiteit voor de logistieke dienstverlener. De doorroutering op het BRIN4 niveau zou dan kunnen plaatsvinden via WS-Addressing headers.

Impact toepassing ODOC: Het voorschrift om ODOC certificaten toe te staan maakt Edukoppeling op dit vlak in mindere mate interoperabel met de Digikoppeling standaard.

PKI certificaten

Edukoppeling heeft de identificatie en authenticatie van een organisatie conform Digikoppeling ingericht op basis van PKI certificaten. Dit kunnen zowel PKIOverheid als ODOC certificaten zijn. Het technische formaat van het ODOC certificaat is vergelijkbaar met die van PKIoverheid. Voor ODOC is ook in grote mate het PvE (deel 3b) van PKIoverheid gevolgd. In de context van een PKI infrastructuur zijn ze echter verschillend. We hebben te maken met verschillende stamcertificaten en organisaties die ze in de rol van TSP[1] uitgeven en ondertekenen. Hiermee is de hiërarchie ervan verschillend en moet er bij het verifiëren van een certificaat de ODOC of PKIoverheid hiërarchie gebruikt worden. Het voordeel van PKIoverheid hiërarchie is dat deze standaard in de (meeste) platformen worden opgenomen, zodat hiervoor geen extra effort noodzakelijk is. Voor ODOC certificaten is hiervoor wel extra inspanning vereist.

Partijen kunnen bij verschillende TSP's PKIoverheid certificaten afnemen, elke TSP stelt (net als PKIoverheid voor de stamcertificaten) een CRL beschikbaar met ingetrokken certificaten. Alleen

[1] TSP (Trust Service Provider). Voorheen ook wel CSP, maar veranderd i.v.m. eIDAS verordening

DUO geeft ODOC certificaten uit en stelt een eigen CRL beschikbaar (ook voor het stamcertificaat). Partijen moeten vertrouwde certificaten controleren tegen de CRL van de CSP die deze heeft uitgegeven.

Impact toepassing ODOC: Er zal extra effort nodig zijn om een platform te voorzien van de ODOC hiërarchie en toetsen of dit correct werkt. Er moet een ODOC CRL gecontroleerd worden, maar dit is een impact die ook zou ontstaan als er een nieuwe partij PKIoverheid certificaten gaat uitgeven.

Toekomstvastheid ODOC certificaten

De ODOC certificaten worden door DUO in het kader van een wettelijke uitvoeringsregeling verstrekt. Deze was echter gebaseerd op de oude situatie waarbij scholen zelf een certificaat aan SaaS-leverancier leverde (eerste scenario). Er waren hierbij vele certificaten nodig (elke onderwijsinstelling minimaal één) en er was hiermee een valide business case.

Volgens het tweede scenario (zie Context) kan men stellen dat ook op langere termijn een behoefte aan ODOC certificaten blijft bestaan (hoewel in dit scenario dus ook mogelijk een PKIoverheid certificaat gebruikt kan worden). Het is overigens meer waarschijnlijk dat er meer en meer volgens het derde scenario gewerkt gaat worden waarbij een SaaS-leverancier een PKIoverheid certificaat gebruikt zoals OSO nu besloten heeft.

Impact toepassing ODOC: Met de nieuwe werkwijze volgens Edukoppeling architectuur en een SaaS-leverancier als logistieke dienstverlener is het benodigde aantal certificaten zeer beperkt. Het is dan ook de vraag of het op de lange termijn leveren van ODOC certificaten als een zinvolle dienst kan worden beschouwd. Naast DUO zelf hebben ook externe partijen de vraag of dit niet als een tijdelijke oplossing gezien moet worden, waardoor men op termijn toch over zal moeten gaan op PKIoverheid certificaten. Partijen configureren liever de systemen op een bestendige manier. Zeker als deze ook beter aansluit op toekomstige ontwikkelingen.

Ontwikkelingen PKIoverheid

De ODOC certificaten sluiten zoveel mogelijk aan op de eisen uit ETSI TS 102 042 en het Programma van Eisen (PvE) PKIoverheid deel 3b. Hiermee is op een bepaald moment een goede aansluiting gevonden met PKIoverheid, maar er blijven op dit punt ontwikkelingen. Er is ondertussen een nieuwe versie (4.4) van het PvE van PKIoverheid gepubliceerd. De impact hiervan lijkt beperkt en is ook enkel ter illustratie bedoeld dat PKIoverheid in beweging is en blijft en dat het volgen hiervan de nodige inspanning vereist en mogelijk impact op ODOC certificaten heeft.

Een andere ontwikkeling bij PKIoverheid is de overgang van G2 certificaten (hiërarchie) naar G3 certificaten (hiërarchie). De G2 (SHA-256) bevat de volgende domeinen:

1. Organisatie
2. Burger
3. Autonome Apparaten

De G3 (SHA-256) bevat de volgende domeinen:

1. Organisatie Persoon
2. Burger
3. Organisatie Services
4. Autonome Apparaten

In 20202 zullen de G2 certificaten vervallen doordat het G2 CA certificaat (onderdeel hiërarchie) verloopt. TSP’s zijn nu ook al begonnen met het uitgeven van G3 certificaten om een geldigheidsduur van drie jaar voor certificaten te kunnen bieden. Partijen in de Digikoppeling/Edukoppeling keten zullen dus nu al de G3 hiërarchie moeten opnemen in hun platformen. Zoals bij G2 zal dit in meeste gevallen automatisch gaan, maar alleen indien men de juiste updates heeft uitgevoerd. Dit laatste is dus enkel een aandachtspunt dat los staat van de

ODOC discussie, alhoewel ook dit de vraag doet rijzen in hoeverre de ODOC certificaten aansluiten bij G3 certificaten. Mocht dit niet zo zijn, dan is hierin een soortgelijke overgangsfase gewenst zoals PKIoverheid toepast.

Impact toepassing ODOC: Dit aspect heeft niet direct impact. Het geeft enkel aan dat het kunnen blijven leveren van certificaten de nodige aandacht blijft vragen en kosten met zich mee zal brengen. Het hangt dus ook samen met het vorige punt, wil DUO in deze dienst blijven investeren.

Ontwikkelingen toepassing op nationaal niveau

Meer en meer nationale standaarden en stelsels schrijven het gebruik van PKoverheid certificaten voor. Indirect wordt vanuit Europese wetgeving (eIDAS) ook meer en meer gestuurd op gestandaardiseerde beveiligingsmaatregelen (web sites beveiligen met een PKIoverheid certificaat). Voor websites die met een browser worden benaderd zal dit in meeste gevallen een ander type (Extended Validation SSL) certificaat betreffen, maar ook dit geeft aan dat er meer en meer convergentie zal komen en dat men gebaat is bij aansluiting op beveiligingsmaatregelen uit andere domeinen.