Memo

Aan: Werkgroep Edukoppeling

Van: Gerald Groot Roessink (DUO)

Betreft: PKI in het PO

Datum: 7 september 2015

Inleiding

Voor uitwisseling van gegevens worden PKI-certificaten gebruikt om de identiteit van de ketenpartner vast te stellen, de vertrouwelijkheid en integriteit tijdens transport te garanderen en een digitale handtekening te zetten. Voor DUO geldt in elk geval dat die certificaten aan bepaalde normen moeten voldoen. Om die reden heeft DUO de afgelopen periode een professionele PKI-infrastructuur opgezet voor het ministerie van OCW. De certificaten zullen vanaf september gefaseerd uitgerold gaan worden gecombineerd met het toepassen van Edukoppeling. Ook andere processen en toepassingen, zoals OSO, waarbij DUO niet een functionele rol heeft, kunnen in principe hun zekerheden baseren op deze PKI-certificaten. Aan de orde is de vraag hoe dat in het Primair Onderwijs (PO) kan worden uitgerold.

Richting VDOD is inmiddels door DUO actie uitgezet over de vraag wat nu wel of niet toepasbaar is op korte termijn. Ook is het onderwerp vorige week aangekaart in de Kerngroep ROSA. De werkgroep heeft in het belang van alle stakeholders een nadere analyse gevraagd. Om die reden vragen we de reacties van de werkgroep Edukoppeling zodat we die weer kunnen verwerking richting Kerngroep en het overleg met de VDOD.

Achtergrond

Beveiligingstechnisch worden er door DUO twee expliciete eisen gesteld aan de uitwisseling tussen DUO en scholen:

- Het certificaat dient te voldoen aan eisen ten aanzien van het soort (X.509) en de robuustheid van de toegepaste algoritmen voor encryptie en signing. De nieuwe invulling daarvan is gebaseerd op PKI-overheid en de toepassing daarvan door Digikoppeling.
- Indien privacygevoelige gegevens door DUO worden verstrekt dan dient de identiteit van de ontvanger met voldoende zekerheid te zijn vastgesteld en dient het doel waarvoor die verstrekking plaats vindt expliciet te zijn gemaakt. In de praktijk is de ontvanger vaak een SAAS-leverancier die namens een school opereert.

Beide eisen zijn verwerkt in wat we het SAAS-model zijn gaan noemen en gelinked is aan de Edukoppeling standaard:

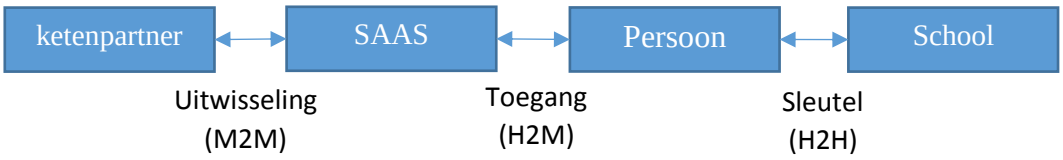
- De school sluit een bewerkersovereenkomst met een gecertificeerde SAAS-leverancier en meldt het bestaan van een mandateringsrelatie via een serviceregister of rechtstreeks bij de ketenpartner.

- De ketenpartners wisselen uit conform Edukoppeling, de school staat als eindontvanger of –leverancier op de SOAP-enveloppe. Een SAAS-leverancier routeert daarmee ‘achter de voordeur’.
- De SAAS-leverancier hanteert een PKI-certificaat op eigen naam voor aanroepen van ene service. De webserviceverlener bepaalt daarmee de identiteit en controleert het bestaan van een mandateringsrelatie.
- Indien de SAAS-leverancier namens de school een webservice verleent bijvoorbeeld voor het aanleveren van gegevens, roept de ketenpartner die service aan op een adres dat uit de mandateringsrelatie volgt.

Hieronder wordt geanalyseerd waarom de huidige uitwisseling in het PO niet meer voldoet aan de gestelde eisen. Geen moment te vroeg heeft DUO een nieuwe en moderne PKI voorziening in productie genomen. Hiermee kan de beveiliging worden aangescherpt.

Afbakening

Beveiliging omvat een veelheid aan aspecten. Hier onderkennen we drie gebieden samen het beveiligingsniveau bepalen:



Toelichting:

1- Uitwisseling
   Bedoeld wordt de uitwisseling tussen systemen van verschillende organisaties met als bijzonderheid dat vaak systemen die het onderwijs ondersteunen vaak in de cloud staan (SAAS). PKI-certificaten worden gebruikt voor veilige uitwisseling.
2- Toegang
   Hier gaat het erom dat leerlingen, leerkrachten of ondersteunend personeel kunnen inloggen tot een (cloud-)systeem. Dit gebeurt vaak met gebruikersnaam en wachtwoord en steeds vaker met meer geavanceerde middelen als SMS of tokens. Er zijn federatieve en ‘eigen’ authenticatiemiddelen in omloop.
3- Sleutel
   Er is er maar één die kan en mag bepalen wie waarvoor toegang krijgt tot het (cloud-) systeem en dat is de school zelf. Die kent een identiteit toe, houdt daar een administratie van bij en moet zorgen dat er sleutels zijn en dat die netjes worden beheerd.

Het onderwerp van deze analyse is een betere beveiliging van het M2M verkeer en kan los worden gezien van de beveiliging van het portaal (H2M) en de sleutel (H2H).

Probleemstelling

De huidige situatie in BRON-PO heeft de volgende karakteristieken:

- Er is een certificaat per school uitgedeeld door DUO. Deze certificaten zijn verouderd, dat wil zeggen volgens gangbare praktijk te eenvoudig te kraken met brute rekenkracht. Verder wordt het uitgifteproces niet meer ondersteund. Dit houdt in dat er geen garanties kunnen worden gegeven dat partijen tijdig over een vervangingscertificaat kunnen beschikken. In het ergste geval betekent dit dat scholen gegevens niet kunnen aanleveren aan BRON.
- Deze oplossing wordt niet door DUO-beveiliging geaccepteerd voor uitwisseling van persoonsgegevens. Hiertoe worden gerekend BRON, VSV en Facet. Alleen voor BRON-PO worden oude certificaten tijdelijk gedoogd met als aanbeveling die dat zo snel mogelijk vervangen dienen te worden. Dat is een belangrijke reden dat OCW opdracht heeft gegeven voor een nieuwe PKI-voorziening die meervoudig bruikbaar is. Die is nu operationeel, maar nog niet uitgerold in het PO.
- Het ontwerp van BRON-PO dateert van voor de opkomst van cloud-computing en is gebaseerd op het idee dat elke school lokaal een certificaat installeert. Die certificaten worden nu vaak doorgegeven aan de SAAS-leverancier waar ze eigenlijk niet voor zijn bedoeld. Voor ketenpartijen is hierdoor niet zichtbaar wie de SAAS-leverancier is die namens een school als bewerker optreedt. De beveiligingsnorm is dat DUO in zo'n geval geen persoonsgegevens mag leveren zoals bijvoorbeeld bij Facet of VSV en ook in BRON. De PGNO-identificatieservice voldoet niet aan die beveiligingsnorm.

Voor DUO zijn dit redenen om de vervanging van de huidige certificaten op de agenda te zetten.

Alternatieven:

De volgende mogelijkheden zijn of worden onderzocht om de beveiliging van vertrouwelijke uitwisselingen op korte termijn te verbeteren met behulp van de nieuwe PKI-certificaten:

1. Vervang alle 7000-8000 certificaten in het PO
   Voor alle Po-scholen wordt een PKI-certificaat ter beschikking gesteld die de SAAS-leverancier zal implementeren. De distributie is een verandering. Dat moet via het Zakelijk Portaal en door in te loggen met een door DUO verstrekt beveiligingstoken.

   Voordeel
   - Op middellange termijn zijn tokens herbruikbaar als DUO- of eventueel sector voorziening.
   - Veranderingen aan de uitwisseling zijn vrijwel verwaarloosbaar.

   Nadeel
   - De aanschaf van tokens is een dure zaak en de distributie is een forse hoeveelheid werk voor DUO, school en SAAS-leverancier.
   - In deze kale vorm geen oplossing voor het niet kunnen leveren aan een onbekende partij. Kan eventueel worden ondervangen met een bewerkersovereenkomst met een gecertificeerde SAAS-leverancier (net als in optie 2).

- Voldoet niet Edukoppeling

2. Hanteer één certificaat per SAAS-leverancier
   Dit is het eerder geschetste SAAS-model (Edukoppeling standaard). De SAAS-leverancier heeft een certificaat op eigen naam. Daarnaast zijn er extra maatregelen nodig die de 'interne keten' tot en met de klantomgeving beschermen.

   Voordeel
   - Langjarige bescherming van het gegevensverkeer
   - Is direct toepasbaar voor toekomstige toepassingen als VSV, Facet, OSO.
   - Voldoet aan Edukoppeling

   Nadeel
   - Nieuw programma van eisen voor huidige situatie BRON-PO

De operatie vervangcertificaten kan voor de scholen die in de cloud werken in beide gevallen vrijwel onzichtbaar zijn. In het eerste geval verlopen de certificaten administratief nog via de school. In het tweede geval kan de vervanging operationeel buiten de school om.