Memo

Aan: Regiegroep OSO
Datum: 7 januari 2016
Van: Marjan Frijns
Onderwerp: Voorstel wijziging PKI infrastructuur OSO

Aanleiding:
Binnen OSO speelt de kwestie van het vervangen van de huidige OSO certificaten (10.000+ verdeeld over 7000+ scholen) die worden gebruikt bij het beveiligen van de communicatie (beveiliging gegevens en identificeren van de afzender en ontvanger ervan). In het laatste technische overleg is een voorstel ingediend om de OSO PKI-infrastructuur te herzien, waarbij het aantal certificaten wordt terug gebracht en het beveiligingsniveau gelijk blijft. Dit wordt bereikt door de huidige OSO certificaten te vervangen door één SAAS-certificaat per leverancier (PKI-overheid certificaat).

Een aantal leveranciers in de OSO keten heeft tijdens het technisch overleg hun zorgen geuit over het afschaffen van de OSO certificaten. Ze zijn niet overtuigd dat de 'SAAS certificaat' variant juridisch overeind blijft. Dat het technische beveiligingsniveau gelijk blijft is hen duidelijk. Maar zij geven aan dat bij een audit zij 'voor de bijl gaan' omdat de (technische) vastlegging van de 'mandateringsrelatie' tussen school en leverancier verloren gaat met het afschaffen van het OSO certificaat.
Naar aanleiding van de gevoerde discussie kwamen drie vragen naar voren die we in dit memo proberen te beantwoorden:

1. Wat doen de OSO certificaten nu binnen OSO, en hoe wordt dit afgedekt in de nieuwe situatie?
2. Welke verantwoordelijkheid gaan leveranciers dragen in de nieuwe situatie en hoe wijkt die af van de huidige?
3. Liggen de gevraagde aanpassingen voor schooljaar 2016/2017 wel in lijn met de landelijke ontwikkelingen of zijn het tijdelijke oplossingen.

Ad 1: Wat doen de certificaten nu binnen OSO?

Binnen OSO zijn er twee typen certificaten: client en server certificaten:

- De server-certificaten zijn 'eigen' certificaten van leveranciers die niet door OSO worden uitgegeven. Een server-certificaat bevat metadata waarmee de betreffende server uniek geïdentificeerd kan worden, bijvoorbeeld de domeinnaam of organisatie van de eigenaar. Een server-certificaat is ondertekend door een publiek erkende Certificate Authority. Hiermee is de identiteit van de entiteit onweerlegbaar vastgesteld. Met een server-certificaat identificeert de server waarop het LAS draait zich in de OSO keten. Deze certificaten worden ook gebruikt bij de versleuteling van de OSO lijnen. De servercertificaten zijn belangrijk voor de beveiliging en het gebruik hiervan in OSO zal niet worden aangepast. Daarom zal dit type certificaat hieronder niet verder besproken worden.
- Client certificaten worden door Kennisnet uitgegeven specifiek voor OSO. Zij worden hieronder verder aangeduid met 'OSO certificaat'. Dit zijn de certificaten die komend jaar vervangen moeten worden. Zij worden gebruikt om de identiteit van een klant systeem aan te geven bij een server. Een voorbeeld hiervan is als een LAS zich aanmeldt bij het Traffic Center; in dat geval gebruikt het LAS haar OSO certificaat om zich bekend te maken. Bij het grote aantal certificaten dat moet worden vervangen gaat het in alle gevallen om de OSO certificaten.

Binnen OSO wordt iedere combinatie van school(vestiging) en het op de school gebruikte systeem geregistreerd zodat dossiers van en naar het juiste schoolsysteem verstuurd kunnen worden. Een

dergelijke koppeling van schoolsysteem met OSO wordt aanleverpunt (AP) genoemd. In OSO krijgt ieder aanleverpunt haar eigen OSO certificaat. Een schoolmedewerker 'geeft' het OSO certificaat aan de leverancier van het schoolsysteem, zodat het schoolsysteem kan koppelen namens de school met OSO.

De OSO certificaten worden nu binnen OSO toegepast om een aanleverpunt te authentiseren. Doordat alle leveranciers hun systemen als SAAS aanbieden, hebben zij meerdere scholen binnen één systeem als klant. Dit betekent dat zij meerdere OSO certificaten binnen één omgeving beheren en opslaan.

Een leverancier met meer scholen als klant en daarmee meerdere OSO aanleverpunten heeft doorgaans voor al deze aanleverpunten één internetadres. Op dit adres zijn meerdere OSO certificaten aanwezig, voor iedere klant één. De klant kiest het OSO certificaat van een specifiek aanleverpunt van een klant om zich te authentiseren op OSO.

Naast het authentiseren op basis van de OSO certificaten wordt in OSO bij iedere overdracht de aanleverpunten van bron- en doel- systemen gecontroleerd tegen het Register. In dit Register is opgeslagen welke aanleverpunten actief zijn. De informatie over de aanleverpunten wordt beheerd door de schoolbestuurders in mijnOSO. Het is de verantwoordelijkheid van de school om aan te geven welke leverancier namens haar mag uitwisselen (als bewerker mag optreden).

Met de controle op basis van het register wordt gecontroleerd of een systeem namens een school een dossier mag opvragen of uitleveren. De authenticatie met een OSO certificaat van een aanleverpunt is eigenlijk 'dubbelop'. Als in het Register het aanleverpunt van de school inactief is of ontbreekt, wordt de uitwisseling gestopt.

In de nieuwe situatie

Bij het invoeren van een SAAS certificaat per leverancier ter vervanging van de huidige OSO certificaten krijgt iedere leverancier één eigen certificaat op haar internetadres. Hiermee wordt de SAAS geauthentiseerd op OSO.

Het voorstel om over te stappen van OSO certificaten naar SAAS-certificaten heeft geen invloed op de verantwoordelijkheid van leveranciers binnen de OSO keten. Het beveiligingsniveau blijft gehandhaafd doordat de controle op toegang tot de OSO keten via het Register blijft lopen. Ook blijft het de taak van de scholen om de aanleverpunten te beheren.

Met het SAAS certificaat wordt de leverancier geauthentiseerd. Op basis van deze controle worden alle aanleverpunten die deze leveranciers namens scholen heeft, toegelaten op OSO. De controle van de aanleverpunten van bron- en doel- systemen tegen het Register blijft. Bij iedere overdracht wordt nog steeds gecontroleerd of een systeem namens een school een dossier mag opvragen of uitleveren.

De SAAS certificaten worden uitgegeven door een vertrouwbare partij namens PKI Overheid. Deze moeten door de leveranciers worden aangeschaft en geïnstalleerd door de LAS leverancier. Scholen staan geheel buiten deze procedure.

<u>Benodigde technische aanpassingen voor overgang naar nieuwe situatie:</u>
Leveranciers van bron- en doel-systemen moeten in hun code de huidige controle van het OSO certificaat vervangen met code voor het controleren van een SAAS certificaat. De impact is (waarschijnlijk) relatief klein doordat de controle niet sterk zal afwijken en er vanuit de

Proefopstelling Edukoppeling voorbeeld code beschikbaar zal worden gemaakt. Of die impact voor leveranciers inderdaad beperkt is willen we tijdens het technisch overleg op 14 januari 2016 vaststellen.
Daarnaast moeten leveranciers een PKI Overheid certificaat aanschaffen en implementeren.

Naast aanpassingen aan de bron- en doel- systemen moeten ook het Traffic Center en het mijnOSO-portaal worden aangepast.

Ad 2.:Welke verantwoordelijkheid gaan leveranciers dragen in de nieuwe situatie en hoe wijkt die af van de huidige?

Leveranciers geven aan dat zij de OSO certificaten (en in sommige gevallen ook school-certificaten uitgegeven door DUO) toepassen om aan te tonen/vast te leggen dat de desbetreffende school de leverancier heeft gemandateerd om namens haar te handelen. Dit is een toepassing die buiten het OSO domein ligt.

Om toegelaten te worden op OSO moet een leverancier zich laten kwalificeren. Hierbij wordt getoetst of de leverancier binnen de scope van OSO valt en of aan het OSO programma van eisen is voldaan. Dit betreft voornamelijk eisen op het gebied van functionaliteit en beveiliging. Ook scholen die op OSO willen aansluiten worden gekwalificeerd. Deze kwalificatie staat los van die van de leveranciers.

Bij het aansluiten en kwalificeren van een schoolbestuur op OSO, wordt er een bewerkersovereenkomst gesloten. Om de kans op fouten te beperken wordt de overeenkomst toegezonden naar het adres van het bestuur of school dat bekend is bij DUO. Bij deze stap is er sprake van identificatie: hierbij wordt bepaald welke school of bestuur wil aansluiten op OSO. Van authenticatie is geen sprake: los van de adrescontrole, wordt er niet gecontroleerd of de school of bestuurder is die bij beweert te zijn. Op basis van het retour ontvangen van de getekende overeenkomst, krijgt de bestuurder toegang tot Mijn OSO, zonder dat hier “role based access control” mogelijk is. Hierna wordt de mogelijkheid geboden het certificaat te downloaden. Bij deze vorm van autorisatie wordt er dus alleen gehandeld op basis van het retour ontvangen van de overeenkomst.

Het certificaat wordt in het verdere proces alleen gebruikt voor identificatie-doeleinden, authenticatie met het certificaat is niet mogelijk aangezien het certificaat een ‘fysiek bestand’ is waarbij de verspreiding en gebruik niet verder is gereguleerd. Bij iedere uitwisseling wordt bij het Register gecontroleerd of de school of bestuur nog geautoriseerd is om bestanden uit te wisselen: bij deze autorisatie wordt het certificaat niet gebruikt.
Het blijkt dat leveranciers het certificaat gebruiken om vast te stellen dat de school of bestuur gerechtigd is om OSO te gebruiken. Hierbij leunt de leverancier op het I(A)A-proces van OSO. Het certificaat is niets anders dan een technisch bewijs dat OSO een bewerkersovereenkomst heeft ontvangen (terwijl een realtime controle alleen plaatsvindt tegen het Register). Hierbij wordt geheel ten onrechte voorbij gegaan aan de rol van de leverancier als bewerker van de school. Zoals volgt uit de WBP, mag een leverancier alleen handelen in opdracht van de school of bestuur. Dat betekent dat in de lijn van het privacy-convenant, de school eerst dit doeleinde moet toevoegen in de bewerkersovereenkomst en privacy-bijsluiter.

Juridisch gezien is er voor leveranciers voor hun eigen product, geen grondslag voor het gebruik van een door OSO gebruikt certificaat. Een leverancier zal altijd zelf een proces moeten inrichten dat de toestemming (instructie) voor aansluiting op en uitwisseling van bestanden via OSO wordt

toegestaan. Het wegvallen van het certificaat is daarbij niet relevant: de leverancier moet sowieso zijn bewerkersovereenkomst met de school wijzigen.

Voor zover de leverancier het certificaat gebruikt om vast te stellen dat de school of bestuur gerechtigd is OSO te gebruiken, is dat gebruik ook onjuist. De verificatie van gebruikersrechten van de school of bestuur (autorisatie), wordt gedaan door een controle tegen het Register (en niet tegen het certificaat). In de relatie school-leverancier, is de bewerker zelf verplicht om direct afspraken te maken met de school of bestuur. Daarbij wordt er vertrouwd op een autorisatie-middel dat buiten de invloeds- en werkingssfeer van de leverancier ligt, en dat is onwenselijk. Als de leverancier al gebruik wil maken van het certificaat, moeten daar met OSO afspraken over worden gemaakt. Gezien de mogelijkheid van 'vrije verspreiding' van het certificaat en het gebrek aan authenticatie, is het gebruik van het certificaat (door leveranciers voor dit doel) een ondeugdelijk middel.

Het gebruik of afschaffen van het certificaat, wijzigt de verantwoordelijkheid van de leverancier niet. Op basis van de WBP is de leverancier immers al verplicht om *zelf* afspraken te maken met de school of bestuur. Dat voor dat doel – ten onrechte – het certificaat werd gebruikt, doet daar niets aan af. De school/bestuur en leverancier moeten het aansluiten op OSO opnemen in de bewerkersovereenkomst en bijbehorende privacy-bijsluiter. Alleen daarmee worden de juridisch noodzakelijke afspraken geregeld. Technisch wordt bij iedere uitwisseling tegen het Register gecontroleerd of de uitwisselende school aangesloten (gekwalificeerd) is op OSO, zodat onrechtmatig gebruik wordt uitgesloten.

Het product van de leverancier wordt door de school of bestuur gebruikt voor meerdere uitwisselingen (ook buiten de OSO-keten zoals uitwisseling met BRON). Het blijft dus van belang dat de leverancier zelf borgt dat de identiteit van de school op de juiste wijze in het product van de leverancier is opgenomen.

Samenvattend: Om de mandateringsrelatie tussen leverancier en school goed te regelen moet in ieder geval komend jaar de bewerkersovereenkomst met bijbehorende privacy bijsluiter worden afgesloten tussen leverancier en aangesloten school. Dit is geen nieuw gegeven en moet, ongeacht de uitkomst van de certificaat discussie, gebeuren.

Ad 3. : Liggen de gevraagde aanpassingen voor schooljaar 2016/2017 wel in lijn met de landelijke ontwikkelingen of zijn het tijdelijke oplossingen.

Hierboven worden twee wijzigingen in de infrastructuur van OSO'16 voorgesteld:

- Het vervangen van de OSO certificaten door SAAS certificaten

De huidige OSO certificaten zijn alleen bruikbaar binnen OSO. Ook wanneer deze certificaten één-op-één vervangen zouden moeten worden (het 10000+ scenario), dan is het niet mogelijk dit zo in te richten dat de OSO certificaten in andere onderwijsketens toepasbaar zouden zijn.

Het uitrollen van het SAAS-certificaat wordt volgens de Edukoppeling standaard uitgevoerd. Dit betekent dat:

- Het SAAS certificaat ook toepasbaar is in andere onderwijsketens die Edukoppeling (gaan) gebruiken
- OSO een stap zet richting Edukoppeling die met een beperkte impact nu een volledige invoering later mogelijk maakt
- Er veel minder certificaten uitgegeven hoeven te worden aan veel kundiger partijen

De verwachting is dat Edukoppeling in de toekomst breed in het onderwijsveld zal worden toegepast. Daarmee is het toepassen van het SAAS certificaat in lijn met de landelijke ontwikkelingen.

Binnen SION is vorig jaar gewerkt aan het certificeringsschema. Aanvankelijk was deze exclusief verbonden aan edukoppeling. In een volgende versie is gekozen voor een breder inzetbaar schema op basis van het ISO27002 normen kader. Op dit moment wordt nog gewerkt aan de invoeringsstrategie. Zodra deze gereed is (eerste helft 2016) kan op basis van deze, in edustandaard vastgelegde, afspraak een risico analyse worden gedaan in de OSO keten. Op basis daarvan worden maatregelen afgesproken. Of deze maatregelen goed door leveranciers (en scholen) zijn geïmplementeerd kan in later stadium onderwerp van een audit en/of certificering worden.

Deze ontwikkeling heeft twee relevante consequenties voor de huidige discussie:

- Overstappen van OSO certificaat naar SAAS certificaat betekent niet dat het certificeringsschema van edukoppeling (en de eventueel bijbehorende audit) automatisch van toepassing wordt.
- We gaan in de keten nog afspraken maken op basis van een risico analyse en het ISO normenkader. Dit gaan we ongeacht de uitkomst van de certificaat discussie doen. Besluit wat we hier nemen heeft er geen invloed op.