

Memo

Aan: Technisch Overleg OSO
Datum: 16 februari 2016
Van: Kennisnet
Onderwerp: Voorstel uitbreiden OSO functionaliteit met Aanleverpunt validatie

Aanleiding:

Tijdens het Technisch Overleg van 16 februari is het voorstel besproken op basis van het [eerder verstuurd memo](#) en een toelichting van Magister. Vanuit de discussie die daarop ontstond zijn er vier alternatieven naar voren gekomen, die hieronder beschreven worden. Wij willen u vragen om deze week (tot en met vrijdag 19 februari 12:00) uw voorkeur door te geven via de techlijst of door een mail naar [ondergetekende](#).

Context:

Vanuit een aantal leveranciers zijn vragen en mogelijke foutscenario's binnen gekomen rond het vervangen van Aanleverpuntcertificaten met SAAS-certificaten. Bij het invoeren van aanleverpunten in Schoolsystemen kunnen gebruikers nu het AP-certificaat gebruiken om de invoer van eindgebruikers te controleren. Deze mogelijkheid vervalt als er geen AP-certificaten meer worden toegepast.

Om tegemoet te komen aan vragen en mogelijke problemen die door leveranciers zijn aangegeven wordt een uitbreiding van OSO met een 'sleutel-controle' van aanleverpunten voorgesteld. Dit biedt een mogelijkheid de invoer van de gebruiker te controleren. De 'sleutel-controle' bewaakt de correcte combinatie van Leverancier (via het SAAS certificaat), BRIN en AP-index. De 'sleutel-controle' biedt geen extra beveiliging of juridische zekerheid(!).

Met deze uitbreiding kan een schoolsysteem een controle uitvoeren op de correctheid van de ingevoerde waarden bij een Aanleverpunt. Hiermee kunnen bewuste en onbewuste gebruikersfouten worden voorkomen.

Keuzen:

Er zijn drie vragen waarop uw antwoord nodig is; deze worden hieronder eerst gepresenteerd. Daarna volgt een uitleg over de 'sleutel-controle' en de vier varianten. Als u de eerste vraag met 'geen' beantwoordt, dan zijn de andere vragen niet meer van belang.

- Vraag 1. Heeft u een voorkeur voor geen, een optionele of een verplichte 'sleutel-controle'?
- Vraag 2. Moet de APsleutel een hashwaarde op basis van een aantal velden of moet het een 'random' karakterreeks zijn?
- Vraag 3. Moet de sleutel alleen worden gebruikt bij het Registeren van een Aanleverpunt of ook bij het aanvragen van een Sessie?

De combinaties van antwoorden leiden tot 3 zinnige keuzes, waarbij opties 1, 2 en 3 ieder twee varianten kennen. In de tabel hieronder wordt de relatie tussen antwoorden en opties weergegeven:

Geen sleutel	Optie 0			
		Nieuwe aanroep	RegistreerAP	+ Sessie Aanvragen
Optionele sleutel	Random	Optie 1random		
	Hash	Optie 1hash		
Verplichte sleutel	Random		Optie 2random	
	Hash		Optie 2hash	Optie 3hash

Optie 0 – Geen ‘sleutel-controle’ optie binnen OSO.

Met de antwoordoptie ‘geen’ bij vraag 1 wordt aangegeven dat u geen sleutel mechanisme in uw systeem wilt inbouwen, maar ook dat u ook niet wilt dat andere leveranciers dit wel inbouwen. Als u geen bezwaar heeft tegen het laten inbouwen door anderen, kies dan optioneel.

Optie 1 – Optionele nieuwe aanroep

In optie 1 krijgt het TC een nieuwe aanroep waarmee de ingevoerde gegevens in het Schoolsysteem gevalideerd kunnen worden. Op basis van de APsleutel wordt gecontroleerd of de waarden voor BRIN, APindex en de Leverancier (op basis van het SAAS certificaat) correct zijn ingevoerd.

Voordeel van deze optie is dat Leveranciers zelf kunnen beslissen deze in te bouwen of niet. Nadeel is dat er verschillen ontstaan tussen de manier waarop Aanleverpunten geregistreerd worden wat verwarrend kan zijn voor eindgebruikers.

Optie 2 – Verplichte sleutel bij het registeren van een Aanleverpunt

In deze optie wordt de bestaande registreerAP aanroep uitgebreid met de APsleutel die verplicht wordt meegegeven naar het TC. Op basis van de APsleutel wordt door het TC gecontroleerd of de waarden voor BRIN, APindex en de Leverancier (op basis van het SAAS certificaat) correct zijn ingevoerd.

Voor en nadeel van deze optie is dat hij verplicht opgelegd wordt. Alle Leveranciers moeten deze inbouwen; daardoor blijft het beheer van Aanleverpunten consistent over alle schoolsystemen heen.

Optie 3 – Verplichte sleutel bij het registeren van een Aanleverpunt én het aanvragen van een Sessie

In deze optie wordt niet alleen bij het registeren van het Aanleverpunt maar ook bij het aanvragen van de Sessie. Dit betekent dat het aanvragen van de Sessie nogmaals de APsleutel moet worden meegegeven en gecontroleerd door het TC. Deze optie is ingebracht door Magister.

Voordeel van deze optie is dat ook bij het aanvragen van een Sessie de controle op de sleutel wordt uitgevoerd. Tijdens het Technisch Overleg werd deze variant met een hash-sleutel acceptabel gevonden, voor de variant met de random sleutel werden de kosten als hoger dan de baten ingeschat. De APsleutel is niets meer dan een verwijzing naar het Aanleverpunt en geeft geen extra informatie die in deze aanroep wordt gebruikt.

Nadeel bij deze optie gekozen wordt voor een random sleutel is een procedure nodig om de huidige aanleverpunten in mijnOSO en bij de Schoolsystemen te vullen met een sleutelwaarde én deze af te stemmen.

Waarde van de sleutel: Random- of hash-sleutel

Opties 1, 2 en 3 komen in twee varianten voor het genereren van de sleutel. Bij de eerste variant wordt een willekeurige tekenreeks als sleutel gegenereerd bij het aanmaken en beheren van een Aanleverpunt. Deze tekenreeks heeft geen extra betekenis en wordt door de eindgebruiker van mijnOSO gekopieerd en ingevoerd in het Schoolsysteem.

In de 'hash variant' wordt de sleutel gegenereerd op basis van een afgesproken 'verhashing' van de BRIN, APindex en Leverancier. Deze hashwaarde wordt gegenereerd in mijnOSO en/of door het Schoolsysteem zelf. Een leverancier heeft daarmee de keuze om de gebruikersinvoer zelf te controleren door de hashwaarde uit mijnOSO te vergelijken met de eigen gegenereerde waarde en/of deze te controleren via de aanroep van het TC.

Bepalen voorkeursvariant

Ik hoop dat u op basis van het bovenstaande (en de eerdere memo's) een voorkeur kunt uitspreken voor een scenario. Mocht u niet tot een keuze kunnen komen of vragen hebben, neem dan contact op met mij via telefoon of email (ik ben woensdag vrij...) of stuur een bericht naar de OSO techlijst.

Groet en dank,

Arjan van Krimpen