Kennisnet

Memo

Aan	Edustandaard werkgroep Edukoppeling
Van	Marc Fleischeuers, ICT-architect, Kennisnet
Datum	26-4-2018
Onderwerp	Bevindingen uit implementaties plus voorstel aanpassingen documentatie Edukoppeling

Op basis van ervaringen bij een aantal projecten (de mutatieservice van SBB, kwalificatietest voor toegang tot de Nummervoorziening, ontwerp van Vroegtijdig aanmelden) zijn er een aantal situaties voorgekomen waarbij de documentatie van Edukoppeling ruimte laat voor interpretatie waarbij er, als partijen verschillende interpretaties kiezen, er geen veilige en succesvolle gegevensuitwisseling plaatsvindt. Bij de interpretaties is de veiligheid van de gegevensoverdracht niet persé in het geding. Het verzoek vanuit de organisaties die te maken kregen met de interpretatieverschillen is om de documentatie van Edukoppeling zodanig aan te passen dat de controles die plaatsvinden bij het valideren van requests en responses uitputtend worden beschreven, voorzien van een classificatie (verplicht, optioneel) en gekoppeld worden aan een beoogd niveau van beveiliging van de verbinding.

De situaties die bij de genoemde projecten voor zijn gekomen, in willekeurige volgorde.

- **Ongewijzigd gebruik van het adres uit de wsa:to header in het http bericht.** Er is een endpoint reference in de wsa:To header, dat sprekend lijkt op het adresveld in de https: headers waar het SOAP bericht in wordt verpakt en getransporteerd. Er zijn implementaties die de endpoint reference in de SOAP header ook gebruiken in de https: header. Dit kan onhandig zijn want de wsa:To header bevat volgens TS 3.4 ook het OIN van de formele partij van het antwoordbericht, dit komt dan ook terecht in de https: header. Dit kan bij de ontvanger weer leiden tot onnodige foutmeldingen, als deze niet rekent op additionele parameters in het request en ze niet kan verwerken.

  De standaarden zeggen weinig hierover, alleen in [SOAP-binding] 3.5 staat “Authors and implementors of bindings should not assume any particular correspondence between native properties and Message Addressing Properties.” (“native properties” staat hier voor properties van het onderliggende protocol).

  Aanbeveling om in de [Transactiestandaard] p9 een zin op te nemen ter verduidelijking, bijvoorbeeld dat de vulling van het http ‘To’ veld waarschijnlijk anders is dan van het wsa:To veld en zeer waarschijnlijk geen oin-parameter zou moeten bevatten.

- **Controle op het TLS certificaat (logistieke laag): hoeft geen PKIo te zijn.** Edukoppeling, net als Digikoppeling, beschrijft het gebruik van certificaten in de logistieke laag (alleen http transport, i.g.v. Edukoppeling) en in de bericht-laag (SOAP bericht). In beide standaarden wordt er weinig expliciet verschil gemaakt in de functie van de certificaten op beide lagen en daarmee de waarde die ze hebben voor beveiligde berichtverkeer. [Transactiestandaard] p9 stelt dat “De gegevensbewerker ondertekent het bericht met een XML-signature (op basis van een eigen PKI-certificaat met OIN).” en “De logistieke dienstverleners kunnen middels de TLS

verbinding geïdentificeerd worden op basis van het certificaat wat hierbij gebruikt is.". In [Edukoppeling Best practices] p10 wordt gesteld dat "In Digikoppeling is ervoor gekozen om PKIoverheid-certificaten te gebruiken op het niveau van het communicatiekanaal (TLS) en de ondertekening en/of versleuteling van berichten.". In de Digikoppeling standaard is dit echter niet terug te vinden; [Gebruik en achtergrond] 2.1.5 zegt "Digikoppeling vereist het gebruik van server (of service) certificaten voor de beveiliging van endpoints van webservices. Voor het signen en versleutelen van berichten wordt aanbevolen om een apart certificaat te gebruiken" en laat hierbij in het midden of op de transportlaag PKIo-certificaten gebruikt moeten worden of niet.
Ik wil er hierbij voor pleiten om expliciet te maken dat er geen noodzaak is voor het gebruik voor PKIo certificaten op transportniveau. De argumenten hiervoor zijn:

1. Beveiligde communicatie op transportniveau voorziet in beveiligd en integer gegevenstransport van point to point. Dat een certificaat afkomstig is uit de hiërarchie van de staat der Nederlanden voegt hier weinig aan toe.
2. De meeste toolkits en/of infrastructuren staan applicatieve controle op dit punt niet toe. Afhandeling van TLS verkeer gebeurt meestal niet door de applicatie die het (payload) bericht afhandelt, en daarmee is controle op de herkomst van het certificaat niet beschikbaar voor de applicatie.
3. In de praktijk van de Edukoppeling berichtuitwisseling gebeurt het niet of vrijwel niet. Ik ben hier zelf mee geconfronteerd toen de Nummervoorziening van een nieuw certificaat werd voorzien, dat afkomstig was van Let's encrypt. Geen enkele aansluitende partij had hier een probleem mee. Op navraag blijkt dat het bij OSO niet gebeurt, en een deel van de fouten die geconstateerd worden bij SBB kunnen alleen verklaard worden als aangenomen wordt dat noch BRON, noch de onderwijsinstelling de herkomst van TLS certificaten valideert.
4. In de documentatie van Edukoppeling en Digikoppeling is niet gespecificeerd dat er een PKIo certificaat op logistiek/transport niveau moet worden gebruikt. Integendeel eigenlijk, de Digikoppeling documentatie 'staat toe' dat een PKIo certificaat voor meerdere doelen mag worden gebruikt, maar alleen als dat handig of goedkoper is ("scheiden van certificaten wordt sterk aanbevolen maar niet vereist").

Mijn **aanbeveling** is om in de documentatie van Edukoppeling expliciet te maken welke verantwoordelijkheid gekoppeld is aan certificaten op bericht- en transportniveau, en daar ook expliciet de controles aan de kant van de ontvanger bij voor te schrijven.

- **Identity check failed for outgoing message**. Treedt op als er een verschil is tussen de CN in het certificaat en de (hostnaam van de) naam van de service, die optreedt zodra een service op virtuele infrastructuur draait (samen met X andere services). Partijen passen verschillende manieren toe om services te combineren achter een certificaat, en de strategie om de naam van een service te valideren (waar we zolang er nog geen goede public key infrastructuur is, nog aan vast zitten) moet hier rekening mee houden.
  Voor Edukoppeling gaat het hierbij om validatie van certificaten op logistiek niveau, waarbij de check uitgevoerd kan worden door infrastructuur, in elk geval buiten de directe controle van de applicatie die het bericht verwerkt. Dergelijke infrastructuur wordt in de regel geleverd door vendors en we verwachten dat internet standaarden gevolgd worden, maar geen eigen (zelfs nationale) standaarden.
  We hebben RFC's [2818], [5280] en [6125] met iets verschillende aanwijzingen over hoe namen van servers te valideren. Ze beginnen in elk geval bij het valideren van de servicenaam in de lijst met subject alternative names (indien aanwezig), en pas als last resort met de CN uit het certificaat. Voor geautomatiseerde clients (M2M) stelt RFC2818 dat er een melding in de log moet worden aangemaakt bij een geconstateerde niet-match, en dat deze client de verbinding ZOUDEN MOETEN (SHOULD) verbreken. Het opstellen van een lijst met alternatieve namen aan de client-kant, zoals hier wel aanbevolen wordt, is niet een erkende

methode volgens de internet standaarden (en dat is ook goed voorstelbaar, gezien het onderhoud aan deze lijst dat door elke client moet worden uitgevoerd!).

Aanbeveling is om de strategie voor de validatie van de server-naam expliciet te maken in de documentatie van Edukoppeling en in lijn te brengen met de relevante internet standaarden, en hierbij SANs in certificaten te betrekken.

- **Firewall afscherming op IP-niveau**. SBB constateert bij het versturen van push-berichten naar instellingen dat een aantal instellingen gebruik maakt van firewalls met white lists voor inkomende berichten op ip-niveau. Nadat het ip-nummer van de dienst van SBB vanwege onderhoud was gewijzigd, kon de dienst een groot aantal berichten niet meer afleveren. Het is evident dat de infrastructuur van instellingen kwetsbaar is, en dat eenvoudige (white list) checks veel doen om ongewenst verkeer buiten te houden. Tegelijk zou het mogelijk moeten zijn om een policy af te spreken waarbij het toelaten van verkeer van erkende partners makkelijker en minder onderhoudsgevoelig is.

  Aanbeveling is om bijvoorbeeld samen met WG IBP en/of TO Continuïteit en beveiliging een passende maatregel uit te werken.

- **Validaties op pushberichten**. De choreografie van request-reply en push-ack berichtverkeer is identiek, maar de semantiek is net omgedraaid: bij request-reply is het informatieve deel van het bericht onderdeel van de reply, terwijl dat bij pushberichten onderdeel is van de push. Voor de ontvanger van een reply (met de gevraagde informatie) is het daarom zinvol om het bericht te valideren op integriteit en herkomst. Voor de verzender van een pushbericht is het een stuk minder zinvol om een acknowledgement van een pushbericht te valideren, de verwerking van de informatie (onderdeel van de push) heeft immers al plaatsgevonden. Wat is de informatieve waarde van een validatie op een ack, en wat zegt het als hierin niet alle berichtvelden gesigned zijn?

  Aanbeveling om in de beschrijving van validaties in de documentatie van Edukoppeling rekening te houden met de semantiek van de transactie, en de informatieve waarde die een validatie oplevert.

- **Berichtheaders bij gebruik van transparante routers**. Bij het ontwerpen van het berichtverkeer in het kader van vroegtijdig aanmelden (waarbij gebruik wordt gemaakt van transparante en niet-transparante routers tussen afzender en bestemming) is gebleken dat het niet gemakkelijk is om berichtverkeer zodanig te adresseren dat zowel routers als afzender en ontvanger hun werk kunnen doen. In Digikoppeling worden voor dit doel de wsa-headers replyTo en faultTo gebruikt. Bij het inrichten van de diensten missen we nu met name de faultTo header. Berichten met fouten in de berichtinhoud (gemeentenummer of PGN niet bekend) worden pas bij de eindbestemming worden ontdekt, en de transacties om de berichten te versturen zijn dan al afgesloten. Dergelijke berichten moeten ofwel via een compleet nieuw in te richten apart kanaal worden verstuurd, of (zoals in deze situatie gekozen) handmatig worden opgevangen en verwerkt in samenwerking met de verzender. Concreet betekent dit voor Kennisnet, voor deze ene dienst, een geraamde maandelijkse inzet van circa 50 uur per maand voor supportmedewerkers.

  Aanbeveling: overweeg het verbod op faultTo op te heffen en documenteer het gebruik ervan in situaties met routering via intermediairs.