FS-20071003.05Cc

OSB Authenticatie

Versie 0.9

Datum: 5 september 2007
DocumentVersie: 0.9

Documentbeheer

Documenthistorie

datum	versie	auteur	opmerking
13 september 2007	0.2	P. Schlotter	Interne afstemversie
2 januari 2007	0.3	P. Schlotter	Besproken in Klankbordgroep OSB, intern GBO, PKI.Overheid
1 maart 2007	0.9	P. Schlotter	Commentaar klankbordgroep en voorstel PKI.Overheid verwerkt

Goedkeuring

datum	versie	goedgekeurd door	opmerking

Inhoudsopgave

1 Inleiding

Dit document beschrijft de uniforme en gestandaardiseerde wijze van authenticeren op de OverheidsServiceBus. De afspraken daarover zijn puntsgewijs opgenomen in hoofdstuk 2. Hoofdstuk 3 en volgende geeft de motivatie voor deze afspraken, d.w.z. achtergrond, analyse, inkadering en nadere invulling.

Terminologie
In dit document worden Engelse termen gehanteerd voor serviceprovider (en dus niet bijv service verlener of service aanbieder) en servicerequester (en niet bijv. service afnemer).

2 Afspraken Authenticatie OSB

Scope:

- OSB richt zich op system-to-system berichtenverkeer (in het kader van gebruik van services) tussen overheidsorganisaties; een uitbreiding (van het stelsel van afspraken) naar organisaties met een publieke taak volgt later.
- Autorisatie wordt beschouwd als een verantwoordelijkheid van de serviceprovider.
- De hieronder beschreven authenticatieafspraken betreffen primair het authenticeren van een servicerequester bij een serviceprovider.

Afspraken:

1. Overheidsorganisaties verlenen toegang tot hun services, die zijn ontsloten via de OSB, aan andere overheidsorganisaties, niet aan resp op het niveau van (individuele) medewerkers van andere organisaties, en niet aan resp op het niveau van applicaties/systemen van afdelingen binnen die organisaties.
2. Dit legt de verantwoordelijkheid voor informatiebeveiliging bij de requesterorganisatie; die dient ervoor zorg te dragen dat servicerequests alleen kunnen worden gedaan door daartoe bevoegde medewerkers en daartoe bevoegde applicaties/systemen.
3. Organisaties authenticeren hun servicerequests bij elkaar d.m.v. PKI.Overheid certificaten. Deze certificaten zijn het middel waarmee de betrouwbare authenticatie (vaststellen van de identiteit) op het niveau van de overheidsorganisatie gebeurt.
4. Wanneer de onder 2 genoemde verantwoordelijkheid bij de requesterorganisatie nog onvoldoende betrouwbaar (gezien de eisen bij de provider) is geïmplementeerd, kan gekozen worden om betrouwbaar te authenticeren op een meer gedetailleerd niveau dan organisatie, d.w.z. wel op het niveau van een afdeling/dienst binnen een organisatie.
5. Wanneer gezien de eisen bij de provider wel met voldoende betrouwbaarheidsniveau (PKI) is vastgesteld dat de request afkomstig is van een betrouwbare organisatie, kan het meer gedetailleerde niveau van afdeling of medewerker meegegeven worden in de payload. Die informatie kan gebruikt worden in de verdere procesafhandeling (vgl “behandeld door”) of zelfs voor autorisatie bij de provider. Afspraken hierover worden gemaakt door dezelfde partijen die ook de overige afspraken over de payload maken.
6. Voor de bepaling van de identiteit van een overheidsorganisatie op de OSB wordt gebruik gemaakt van een uniek identificerend nummer, dat is opgenomen in het HR.
7. Dat identificerende nummer (binnenkort wordt besloten of dat het FI-nummer, dan wel het KvK-nummer is uit het HR) wordt opgenomen in het certificaat, dat vereist is bij gebruik van de OSB. Regels hierover zijn (worden) opgesteld door PKI-Overheid. In

het vertificaat wordt hiervoor gebruik gemaakt van het veld Subject.Serialnumber. Het veld Subject.organisationName bevat de (leesbare) naam van de organisatie. Voor het in punt 4 bedoelde meer gedetailleerde niveau binnen een organisatie wordt gebruik gemaakt van het veld Subject.organizationalUnitName.

8. Er wordt onderscheid gemaakt naar:
    a. authenticatie t.b.v. de autorisatie voor het mogen uitvoeren van een bepaalde servicerequest door een requester (bijv het mogen opvragen van een bepaalde set gegevens, of het mogen aanbieden van een bepaalde transactieaanvraag)
    b. juridisch noodzakelijke authenticatie resp integriteit van een transactie d.m.v. een elektronische handtekening.

   Een dergelijke handtekening voldoet aan veel verdergaande eisen (langjarig bewijs, onwijzigbaarheid van de transactie etc) dan noodzakelijk voor autorisatie alleen; die handtekening kan uiteraard ook gebruikt worden t.b.v. de authenticatie voor autorisatie, maar is de meeste gevallen een te zwaar middel.
   Gekozen wordt daarom om authenticatie t.b.v. autorisatie te scheiden van een handtekening. Authenticatie t.b.v. autorisatie wordt belegd op de logistieke laag; de handtekening bevindt zich in de inhoud.
9. Authenticatie op de logistieke laag kan gebeuren op KANAALniveau (TLS) of op ENVELOPniveau (XMLDsig).
   In OSB versie 1.0 wordt alleen gewerkt met KANAALniveau.
   NB De in het vorige punt genoemde handtekening wordt aangeduid met niveau BERICHT.
10. De hier geschetste wijze van authenticeren geldt voor de servicerequests en de daarmee gepaard gaande uitwisseling van gegevens die vallen onder het regime van WBP klasse 2 (CBP AV23) resp departementaal vertrouwelijk uit VIR-BI. Dit is nog geen eenduidige definitie. Wanneer strengere eisen gesteld worden, resp sprake is van bijzondere gegevens, kunnen andere (inrichtings)eisen bestaan.

3 Achtergronden Authenticatie OSB

Dit hoofdstuk en volgende bevat de onderbouwing van de in hoofdstuk 2 genoemde afspraken.
Dit hoofdstuk bevat een analyse met een aantal uitgangspunten m.b.t. scope van OSB en een aantal begripsbepalingen. In hoofdstuk 4 zijn de conclusies daaruit verwoord, en hoofdstuk 5 bevat de voorgestelde inrichting van authenticatie. Tot slot is in hoofdstuk 6 nog een toelichting gegeven wat die inrichting in een aantal situaties betekent.

3.1 Scope OSB

De OSB faciliteert het gebruik van services (als bedoeld in de Service Gerichte Aanpak in de NORA). Een service wordt aangeboden door een bepaalde organisatie (serviceaanbieder of Service Provider) en afgenomen door een andere organisatie (serviceafnemer of Service Requester). Gebruik van een service gebeurt door uitwisseling van berichten.
Die uitwisseling vereist afspraken op 3 niveaus:

- Inhoud van de uitwisseling resp van de berichten; afspraken worden gemaakt door “business”, en geïmplementeerd in de samenwerkende applicaties;
- Logistiek, afspraken tussen samenwerkende partijen, standaardisatie is doel van de OSB; afspraken voor de logistieke en transportafhandeling worden geïmplementeerd in van business onafhankelijke “adapters”.
- Netwerk, TCP/IP connectivity, afspraken tussen netwerkverantwoordelijken van samenwerkende partijen en tussenliggende netwerken; te standaardiseren op landelijk niveau (BLN)

Over de OSB gaat alleen A2A (administration-to-administration, ook wel system-to-system) verkeer en geen P2A (person-to-administration) verkeer; alleen webservices worden ontsloten en geen portals/websites.

3.2 Authenticatie en autorisatie: Functioneel

Authenticatie en autorisatie is nodig, omdat de serviceverlener in staat moet zijn om de serviceafnemer met voldoende zekerheid (zoals vereist conform WBP, VIR, etc) te kunnen identificeren (authenticatie) om daarmee te kunnen bepalen of die geïdentificeerde afnemer gerechtigd is (autorisatie) tot het uitvoeren van de gewenste service.

Functioneel relevant is vooral de vraag welke identiteit maatgevend is of moet zijn voor de bepaling van de autorisatie (“wie” krijgt toegang tot welke service).

Een ander belangrijke requirement van de OSB is dat servicegebruik en dus berichtenuitwisseling mogelijk moet zijn met een minimum aan maatwerkontwikkeling door

zowel serviceaanbieder als (met name) door de serviceafnemers. Dat betekent dat er keuzes gemaakt moeten worden uit de beschikbare software implementaties van open standaards. Verschillen in authenticatie tussen ebMS en WUS dienen zo veel vermeden te worden op functioneel niveau, en dienen dus zoveel mogelijk beperkt te blijven tot implementatiedetails, zoals codering van specifieke parameters.

In deze notitie blijft vooralsnog een aantal zaken buiten beschouwing:

- De serviceafnemer wil omgekeerd ook zekerheid hebben dat het verzoek terecht komt bij de beoogde serviceverlener; deze “omgekeerde vorm” blijft in deze notitie verder buiten beschouwing.
- Bij autorisatie kan ook sprake zijn van toegang tot slechts een beperkte set van gegevens(objecten).
- Machtiging, dwz iemand initieert een servicerequest namens een ander; het verschijnsel logistieke intermediair (dwz een organisatie verzorgt de logistiek tbv de verantwoordelijke) is wel relevant , zie verder.
- De wijze waarop autorisatie plaats vindt, bijv al of niet gebruik makend van een centrale autorisatievoorziening (waarbij de feitelijke autorisatie-regels de verantwoordelijkheid blijven van de serviceaanbieder).
- Federated Identity Management blijft buiten beschouwing, omdat met de voorstellen in deze notitie vooralsnog geen behoefte bestaat aan federaties.

3.3 Subjecten betrokken bij authenticatie op de OSB

Zoals eerder gesteld is het de verantwoordelijkheid van de serviceaanbieder om een request van een bepaalde requester wel of niet te autoriseren. Deze paragraaf analyseert welke soorten resp niveaus van requesters (subjecten) er in principe zouden kunnen zijn, zodat in het volgende hoofdstuk een voorstel gedaan kan worden welke soort of niveau gekozen wordt op de OSB als de basis voor autorisatie en dus voor authenticatie.

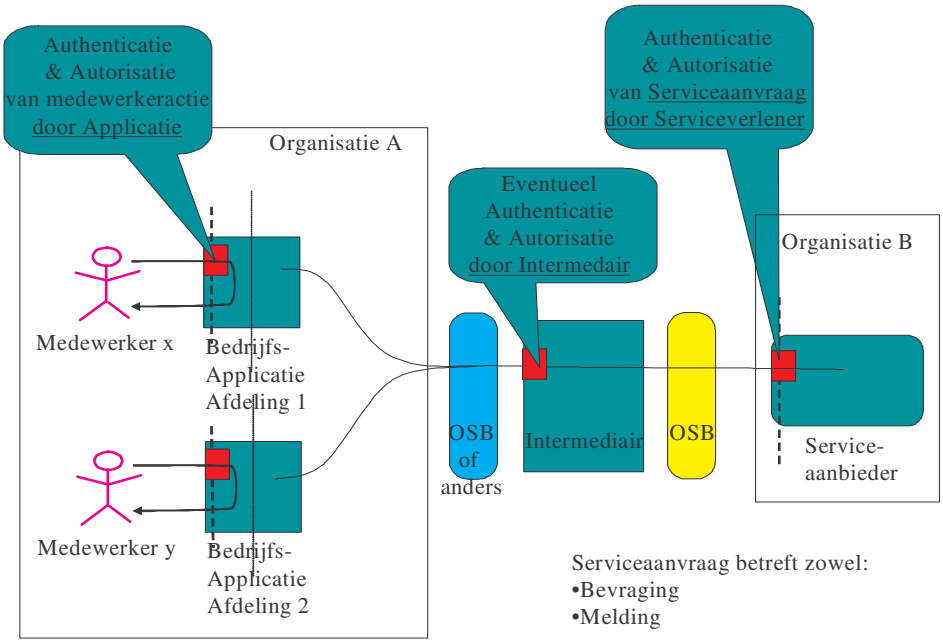
De belangrijkste hoofdsubjecten zijn:

- Serviceafnemer d.w.z. initiërende overheidsorganisatie; die op business-niveau de service afneemt. Direct of indirect moet diens identiteit betrouwbaar bepaald worden door de serviceverlener.
- Intermediair d.w.z. overheidsorganisatie die diensten levert voor deze service of berichtstroom, op het niveau van transport, logistiek en/of inhoud.

Binnen iedere overheidsorganisatie komen nog andere subjecten voor:

- Afdelingen en informatiesystemen; in werkelijkheid zullen binnen een overheidsorganisatie verschillende afdelingen en/of verschillende informatiesystemen verantwoordelijk zijn voor het afnemen van de betreffende service.
- Medewerker; binnen een afdeling/informatiesysteem van een overheidsorganisatie is een medewerker (of een van buitenaf ingelogde burger) verantwoordelijk voor het uitvoeren van taken die leiden tot het afnemen van de betreffende service.

Hierbij is dus sprake van lagen, hierna subjectniveaus genoemd.
In onderstaande figuur is dit weergegeven.



Figuur 1 Niveaus van mogelijke afnemers

De kernvraag bij het bepalen van het niveau waarop een afnemer moet worden bepaald ligt bij de autorisatie. Als bijvoorbeeld door de serviceaanbieder gesteld wordt dat alle serviceaanvragen die afkomstig zijn van de intermediair toegestaan zijn, maar dat nog wel gelogd moet worden welke medewerker de vraag geïnitieerd heeft, dan hoeft kennelijk alleen de intermediair geauthenticeerd te worden.

3.4 Authenticatie en autorisatie in SoftwareLagen

Autorisatie is een verantwoordelijkheid van de serviceverlener. Zelfs als er sprake zou zijn van zoiets als een generieke autorisatievoorziening, blijft de serviceverlener verantwoordelijk voor de invulling van de inhoudelijke regels, en dus eindverantwoordelijk. Uit overwegingen van overzichtelijkheid blijft een dergelijke voorziening vooralsnog buiten beschouwing.

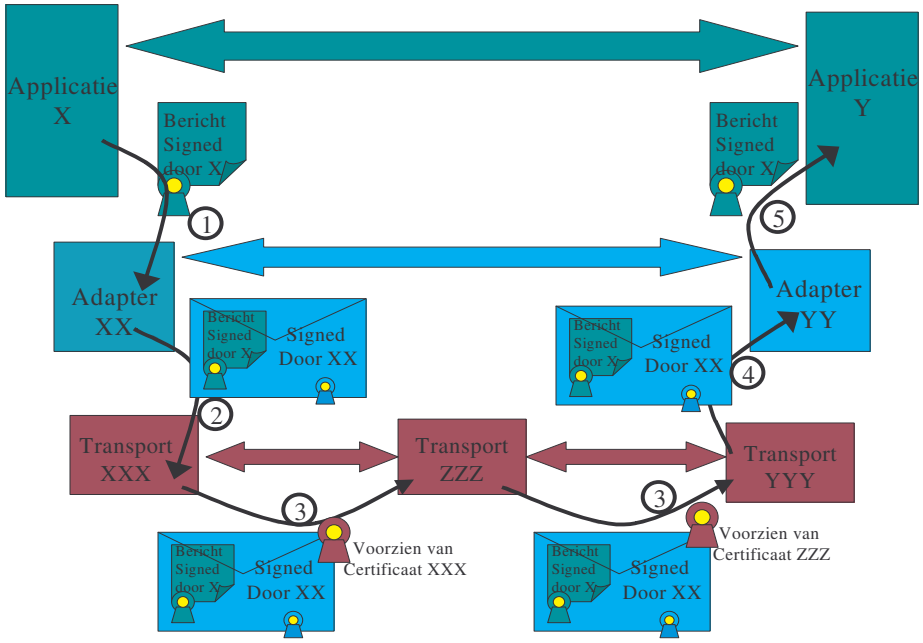
Autorisatie (en dus de daarvoor benodigde Authenticatie, alsmede de daarbij gewenste logging resp. Audittrail gezamenlijk hierna AAA) genoemd is een groep functionaliteit die men graag zo los mogelijk van de feitelijke (business)verwerking in de applicatie wil houden. Dat heeft er toe geleid dat AAA in de ontwikkeling van internationale standaards en daarop gebaseerde beschikbare (standaard)software op diverse lagen is ontstaan:

- op netwerkniveau, VPN, IPSec etc, afgehandeld door hardwarematige netwerkcomponenten; dit niveau blijft verder buiten beschouwing;
- op niveau van het transportkanaal, TLS (SSL), afgehandeld door low-level communicatiesoftware;
- op logistiek niveau, in de SOAP-header (envelop) van een bericht, afgehandeld door (logistieke) adapters;
- op applicatieniveau, in het bericht zelf, afgehandeld door de applicatie, of een generieke deel daarvan.

In principe handelen al deze lagen (conform de bijbehorende open standaards) zelfstandig (een deel van) de authenticatie en autorisatie af. Dat betekent dat iedere laag daarvoor een mechanisme kent, en vooral dat iedere laag alleen berichten doorlaat die door die laag geautoriseerd zijn. Iedere laag verwijdert in principe alle informatie die gebruikt wordt voor de AAA, voordat het bericht wordt doorgegeven aan de bovenliggende vervolglaag. Meestal dienen aanvullende maatregelen (dus niet standaard) genomen te worden om dergelijke informatie toch door te geven.
Overigens wordt altijd gebruik gemaakt van PKI om de identiteit betrouwbaar te bepalen. Het resultaat van die controle kan leiden tot uitgifte van een ticket of token (bijv SAML-token) met een bepaalde geldigheidsduur; verder hierna vooralsnog buiten beschouwing gelaten.
Die identiteit wordt bijv geauthenticeerd door een PKI-handtekening te controleren. Handtekening en identiteitscontrole zijn (bij PKI) sterk aan elkaar gekoppeld.

Deze indeling en werking van de beschikbare software is relevant, omdat de OSB streeft naar een stelsel van afspraken dat geïmplementeerd kan worden met zo min mogelijk maatwerk, en dat dus zoveel mogelijk gebruik maakt van beschikbare software op basis van open standaards.

De diverse mogelijkheden van de lagen en hun relatie zijn samengebracht weergegeven in onderstaande figuur.



Figuur 2 Identiteit in lagen

1. Applicaties maken gebruik van elkaars services door het uitwisselen van berichten. In dit geval stuurt Applicatie X een bericht (servicerequest) naar applicatie Y, eventueel is het bericht zelf getekend door X.
2. Het versturen wordt voorbereid door de “postkamer”, d.w.z. adapter XX, die het bericht inpakt in een envelop. Indien overeengekomen, wordt het bericht op (in) de envelop gesigned door de adapter XX.
3. Die envelop wordt verstuurd door de communicatie- en transportlagen over een transportkanaal, die in het geval dat tweezijdig TLS is afgesproken, een

clientcertificaat toevoegt aan de envelop, die bijv. verstuurd wordt naar een tussenstation ZZZ.

4. Die accepteert het transport afkomstig van XXX, en verstuurt het naar YYY. Die accepteert (dus positieve autorisatie) een transport van ZZZ, verwijdert de TLS-informatie en biedt het resterend bericht, dus de envelop met de signature van XX aan aan de eigen adapter YY.
5. De adapter (postkamer) YY controleert conform het contract de signature van XX, verwijdert de envelop met de signature-informatie en geeft het resterende bericht, signed door X door aan de geadresseerde applicatie Y. Applicatie Y kan vervolgens zorgdragen voor archivering van het bericht met handtekening X, bijv conform W3C XAdES[1].

In de hier geschetste maximale situatie heeft iedere laag een eigen methode om de identiteit vast te stellen en vervolgens te autoriseren; iedere laag bevat dus ook een “autorisatietabel” (ACL, policy/contract, etc). Een andere inrichting kan zijn dat de identiteit die betrouwbaar is vastgesteld op een onderliggende laag wordt doorgegeven (NB na autorisatie, die in het algemeen niet/moeilijk uitschakelbaar is) naar de bovenliggende laag. Een andere mogelijkheid is dat AAA op minder lagen plaats vindt, bijvoorbeeld alleen op op envelop-niveau en niet ook op kanaal-niveau.

De AAA’s die door de verschillende lagen worden uitgevoerd verschillen in bepaalde opzichten, onder andere in niveau van betrouwbaarheid, en vooral in de manier waarop beheer van authenticatie en autorisatie is geregeld .
Een hogere laag geeft in het algemeen gesproken een hoger (want specifieker op het betreffende request gericht) niveau van betrouwbaarheid.
Binnen een laag bestaan ook alternatieven; bijv binnen de logistieke envelop-laag kan geauthenticeerd worden op basis van X509 token (signature), of een SAML-token of nog andere voor de OSB minder voor de hand liggende alternatieven.

In principe moet per service bepaald worden welk niveau vereist is, en dus op welke laag de AAA plaats vindt. Tevens dient een keuze gemaakt te worden voor de authenticatiewijze binnen die laag. De voorstellen in het volgend hoofdstuk beschrijven de beoogde ondersteunde varianten op de OSB, en geven vervolgens handvatten hoe die varianten gebruikt kunnen worden.

3.5 Certificaten en Identiteit

PKI-certificaten zijn direct of indirect de drager van de identiteit. Dat geldt op alle lagen.
Het Programma van Eisen voor PKI.Overheid certificaten geeft een nadere specificatie van de in de standaard X509v3 mogelijk velden.

[1] This note (XAdES) extends the IETF/W3CXML-Signature Syntax and Processing specification [XMLDSIG] into the domain of non-repudiation by defining XML formats for advanced electronic signatures that remain valid over long periods and are compliant with the European "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures" [

Een van de te maken hoofdkeuzes betreft het wel of niet in het certificaat vastleggen van de direct voor authenticatie te gebruiken identiteit van het subject, dus van de overheidsorganisatie met eventuele subniveaus.

PKI.Overheid PvE deel 3b onderkent de volgende eisen aan de diverse subject gerelateerde velden, onderdeel van de DN (Distinguished Name) in een PKI-Overheidscertificaat.

NB dit PvE wordt aangepast als gevolg van de noodzaak om een identificerend nummer op te nemen in het PKI.Overheidscertificaat. Voorstel is hiervoor het veld Subject.serialNumber te gebruiken.

Subject.countryname	C=NL
Subject.commonName	CN= DNS name bij server
Subject.organisationName	O=volledige naam van de organisatieconform (geaccepteerd document of) basisregistratie; voorstel is om hiervoor de naam te hanteren die is voorgeschreven PvE HandelsRegister. Hier is geen nummer toegestaan
Subject.organizationalUnitName	OU= optioneel;
Subject.serialNumber	Nummer van de (overheids)organisatie

Bovenstaande maakt het mogelijk dat een organisatie voor alle servicerequests gebruik maakt van dezelfde identiteit (dus het nummer uit het certificaat).
Wanneer die organisatie bijvoorbeeld zou beschikken over twee rekencentra, dan blijft het gewenst dat die twee centra zich met dezelfde identiteit authenticeren, maar uiteraard met twee verschillende certificaten. Het serialnumber en/of OU zullen verschillen, en dus is er sprake van verschillende certificaten. De autorisatie is echter gericht op dezelfde identiteit. Mogelijk zou de ServiceProvider nog iets kunnen doen met dat onderscheid, maar de strekking van deze notitie is juist om alleen op basis van de organisatie-identiteit (dus “O”) te authenticeren en autoriseren.

Wanneer de eisen van de serviceprovider t.a.v. authenticatie zodanig zijn dat de servicerequester organisaties daaraan (nog) niet kunnen voldoen, kan afgesproken worden om (in het certificaat) ook Subject.organizationalUnitName mede bepalend te laten zijn voor de identiteit van de servicerequester.

4 Conclusies voor inrichting authenticatie op de OSB

In het vorig hoofdstuk zijn lagen en niveau onderkend. Dit hoofd beschrijft de voorstellen voor de te leveren ondersteuning op de OSB.

4.1 Subjectniveaus

- De autorisatie bij serviceaanbieder (organisatie B) is niet afhankelijk van de identiteit van de medewerker van organisatie A. Bij de authenticatie bij de serviceaanbieder speelt de medewerker-id dus geen rol. (Die medewerker-identiteit kan best opgenomen zijn in de payload t.b.v. het proces). De service bij Organisatie B vertrouwt er op (op basis van overeen te komen landelijke aansluitvoorwaarden) dat organisatie A die autorisatie goed geregeld heeft.
- De autorisatie bij de serviceaanbieder is ook niet afhankelijk van informatiesysteem (applicatie) of afdeling van waaruit de aanvraag ontstaat. De service bij organisatie B vertrouwt er op (aansluitvoorwaarden) dat organisatie A goed geregeld heeft dat alleen de daartoe gerechtigde afdeling/informatiesysteem de betreffende serviceaanvraag genereert.
  Onderkend wordt dat dit een gewenste situatie is, die nagestreefd zou moeten worden, maar in thans in bepaalde situatie nog niet gehaald kan worden. Uitbreiding naar het afdelingsniveau is dan toegestaan.
- De serviceaanbieder B beoordeelt dan alleen of de betreffende serviceaanvraag toegestaan is voor organisatie A (resp in bepaalde situaties voor afdeling X binnen Organisatie A).

4.2 Belegging AAA op Uitwisselingslagen

De service bepaalt het vereiste authenticatieniveau, en daarmee dus op welke laag AAA plaats vindt. Er worden vier niveaus onderkend:

- TLS-1: Alleen TLS, ook via intermediairs
  Toepasbaar voor services, waarbij een keten van trust inclusief intermediairs voldoende is. Dit kan van toepassing zijn voor situaties waarbij er weinig eisen gesteld worden aan de service (bijvoorbeeld het “mogen” aanbieden van een terugmelding), maar ook bij een expliciet afgesproken rol van de intermediair (bijv bevragingen van GBA door scholen/instellingen via IBG. GBA autoriseert IBG, hoewel de school de eigenlijke bevrager is.
- TLS-2, Alleen TLS, echter geen intermediairs in een trusted rol toegestaan.
  Het verschil tussen TLS -1 en TLS -2 is betrekkelijk gradueel. In beide gevallen dienen afspraken gemaakt te zijn over de rol van de intermediair.
- ENVELOP: AAA op Logistiek niveau, wel eenzijdig TLS voor vertrouwelijkheid;
  Door de authenticatie te beleggen op logistiek envelop niveau is het ongeacht het wel of niet bestaan van intermediairs mogelijk voor de serviceaanbieder om de “echte” serviceafnemer te authenticeren.
  NB1: Zoals in voorgaande paragraaf 1.4 is toegelicht, zal in dit geval de autorisatie

plaats vinden door de standaard software op de logistieke laag.
Eventueel zou een getrapte autorisatie kunnen worden ingericht, waarbij de logistieke laag in feite de requester autoriseert om “enige” service uit te voeren bij die aanbieder, en waarbij de applicatie zelf vervolgens het uitvoeren van een specifieke service authenticeert. Voor de afspraken op de OSB hoeft dat geen verschil te maken. Het is een interne constructiewijze binnen de aanbieder.

- BERICHT, AAA op applicatieniveau, dus in de berichtinhoud; TLS voor vertrouwelijkheid.
  Voor de authenticatie en autorisatie op het moment van uitvoeren van de service zal het verschil met ENVELOP niet groot zijn; in beide gevallen wordt de “echte” serviceafnemer geauthenticeerd, op basis van een certificaat met dezelfde betrouwbaarheid. Voor de langjarige bewijslast heeft BERICHT een voordeel, omdat vanuit de applicatie het getekende bericht langdurig bewaard kan worden. De ondertekening (t.b.v. authenticatie) in het geval ENVELOP wordt in principe door de logistieke laag (adapter) verwijderd en alleen gelogd.
  Standaards en software zijn op dit niveau nog geen gemeengoed.

4.3 Noodzaak voor het doorgeven van identiteitsinformatie naar hogere laag

De SP bepaalt hoe de autorisatie (en logging) wordt ingericht. Wanneer bijv gewerkt wordt met TLS client certificaten, kan de autorisatie belegd worden in de TLS-software, bijv m.b.v. Access Control Lists (ACL). Indien gewenst kan de SP natuurlijk ook de in de TLS-laag vastgesteld identiteit doorgeven aan de achterliggende applicatie, en daar autorisatie inrichten.
Voor het protocol op de OSB wordt uitgegaan van één mechanisme (in dit voorbeeld dus authenticatie m.b.v. een clientcertificaat. Hoe de ontvanger daar mee omgaat is voor de OSB niet van belang.

5 Voorgestelde implementatie

Voor de OSB op de Logistieke laag bestaan er twee implementaties (logistieke profielen), binnen een context van (aansluit)afspraken:

- Profiel KANAAL
  In dit profiel gebeurt de authenticatie d.m.v. TLS een client-certificaat. Door de TLS-laag wordt vervolgens geautoriseerd op basis van het veld “O” (organizationalUnitName) in het certificaat.

  Hiermee worden de bovenstaande niveaus TLS-1, TLS-2 en BERICHT ondersteund. In principe is 2-zijdig TLS niet nodig voor BERICHT, maar uit overwegingen van standaardisatie, en het feit dat daarmee niet geautoriseerde requests op een eerder moment kunnen worden onderschept, pleiten we toch voor 2-zijdig TLS.

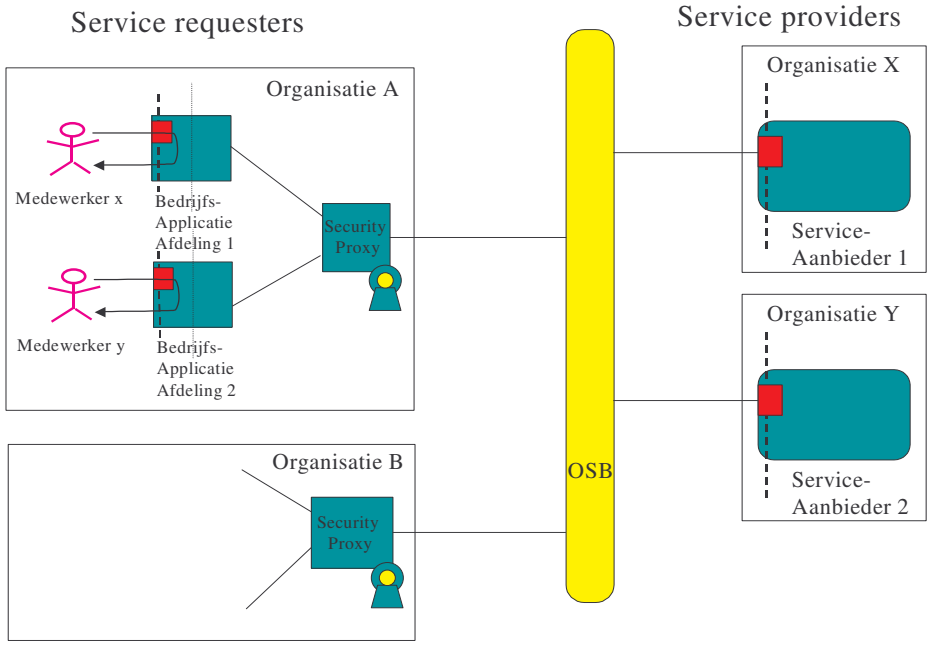
- ENVELOP
  In dit profiel gebeurt de authenticatie door het ondertekenen van (een deel van) het bericht met het certificaat van de afzender. Na controle van de handtekening en het certificaat gebeurt de autorisatie op basis van de inhoud van hetzelfde veld “O” uit dat certificaat. Deze authenticatie is onafhankelijk van eventuele tussenstations.
  De encryptie wordt in dit profiel (tenminste) gedaan m.b.v. TLS

De feitelijke implementatie van BERICHT bevindt zich binnen de payload, dus buiten de scope van de Logistieke laag en OSB. Dit mechanisme wordt in het totaal van de uitwisseling dus wel onderkend, maar maakt geen deel uit van de afspraken op Logistiek niveau

Deze twee implementaties KANAAL en ENVELOP gelden zowel voor bevragingen (op basis van WUS) als voor meldingen (op basis van ebMS).

6 Toelichting bij het gebruik van deze implementatie

Onderstaande figuur 3 schetst de waarschijnlijk veel voorkomende situatie aan de OSB. Er zijn diverse organisaties die services willen afnemen (Service Requesters, SR) en diverse organisaties die services aanbieden (Service Providers, SP).
In de beoogde opzet van de OSB zullen SR en SP rechtstreeks met elkaar communiceren. Logistiek profiel KANAAL kan hier uitstekend worden ingezet; t.a.v. authenticatie is dat voldoende.



Figuur 3 Rechtstreekse communicatie tussen requester en provider

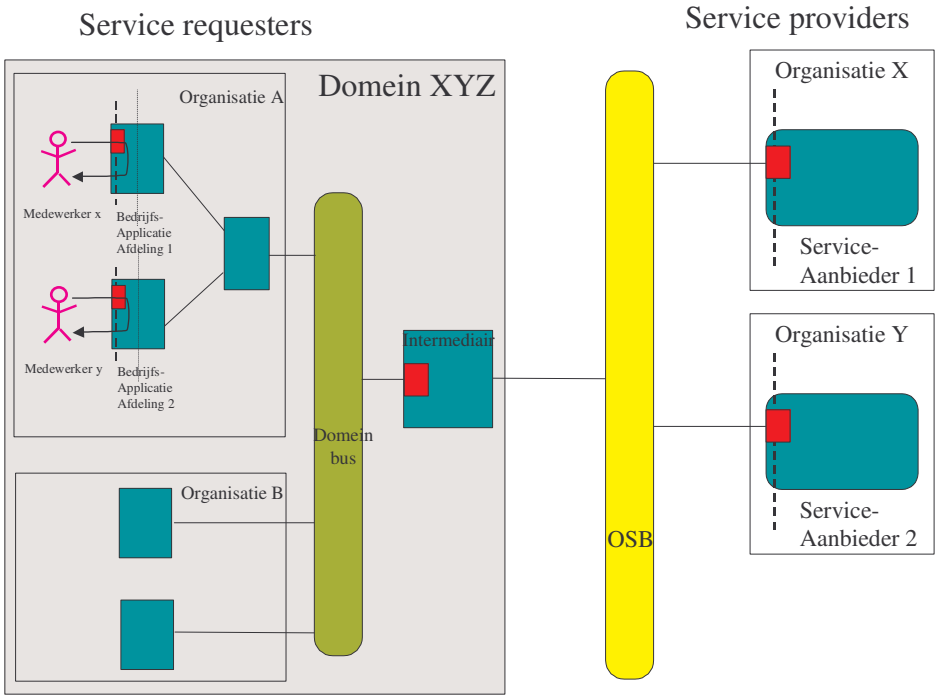
Onderstaande figuur 4 schetst een andere vaak voorkomende situatie. In een bepaald domein XYZ bevinden zich diverse SR's die services afnemen welke zich rechtstreeks aan de OSB bevinden. De wijze waarop binnen het domein de SR's zijn aangesloten aan de eigen domeinbus, is niet relevant voor de OSB, en daarom hier alleen zeer schetsmatig weergegeven. Aan de rand van het domein XYZ bevindt zich een transformatiepunt, een intermediair. Afspraken zullen gemaakt moeten worden tussen intermediair (namens het domein of de sector) en SP's aan de OSB.

Er zijn diverse mogelijkheden:

- de intermediair stelt zich op namens het domein en dan wordt de intermediair geauthenticeerd en geautoriseerd door de SP's; profiel KANAAL tussen intermediair en SP voldoet. Dit gebeurt bijv bij IBG namens scholen/instellingen naar GBA.
- De SP's willen wel de achterliggende organisaties kunnen onderscheiden, autoriseren en dus authenticeren. Dit kan bijv. gerealiseerd worden (zoals bij SUWI) doordat de door de SP erkende authenticatiemiddelen (KANAAL) ondergebracht worden bij de intermediair, die dan vervolgens het juiste middel (certificaat) inzet afhankelijk van de achterliggende organisatie. De intermediair gebruikt de ene keer

(het certificaat met) de identiteit van Organisatie A en de andere keer die van Organisatie B. De SP's dienen uiteraard met deze werkwijze akkoord te gaan.

- De SP's willen de achterliggende organisaties onderscheiden, maar staan de vorige werkwijze niet toe. Wanneer de intermediair en daarmee het KANAAL tussen intermediair en SP wel wordt vertrouwd, kan ook besloten worden om de identiteit van de achterliggende Organisatie in het bericht op te nemen, waardoor authenticatie in de applicatie eenvoudig te realiseren is.
- Wanneer ook dat niet is toegestaan, een profiel KANAAL niet voldoende, maar moet gekozen worden voor ENVELOP.
  Vraag is hoe vaak deze situatie zich werkelijk voor doet.



Figuur 4 Communicatie via een intermediair (ofwel sektorloket voor domein XYZ)

6.1 Bereikbare resultaten

Met de hiervoor geschetste aanpak worden een aantal doelstellingen haalbaar.

- Logisch één certificaat per afnemende organisatie bruikbaar voor alle services: implementeerbaar via bijv. één proxy met "het" certificaat, of via meerdere proxies met verschillende certificaten, die echter allemaal dezelfde O hebben
- Centrale afhandeling van de authenticatie per (afnemende) organisatie (dus bijv via OSB-gateway) wordt bereikbaar (niet noodzakelijk).