



SHIBBOLETH: WAT IS HET, WAT KUN JE ERMEE?

OVERVIEW

INHOUD

Deze factsheet gaat onder andere in op wat Shibboleth is en wat ermee mogelijk is.

Bron: <http://shibboleth.internet2.edu/>

OVER DE AUTEUR

John van Westeneng is Identity & Access management consultant en managing partner bij Traxion.

“Veelal wordt Shibboleth in een adem genoemd met OpenSource initiatieven als A-Select, OpenSAML en OpenLDAP. De relatie met Shibboleth is aanwezig alleen lossen de genoemde initiatieven niet dezelfde problematiek op.

John van Westeneng, CISSP – auteur.

In dit artikel wordt ingegaan op wat Shibboleth is, wat je eraan hebt en wat de relaties zijn tussen Shibboleth en de genoemde OpenSource initiatieven. Het is geschreven om een stuk onbekendheid weg te nemen en meer duidelijkheid te verschaffen over de mogelijkheden van Shibboleth in de Nederlandse Identity & Access Management markt.



Traxion

Traxion is een onafhankelijke System Integrator, gespecialiseerd in Identity Management oplossingen. Met een oplossingsgerichte aanpak begeleiden wij onze cliënten van idee naar een volledige Identity Management oplossing. Onze belangrijkste succesfactor bestaat uit de juiste combinatie van ervaring, kennis, deskundigheid en professionaliteit.

Sinds 1997 hebben Traxion specialisten voor gerenommeerde multinationals een groot aantal Identity Management oplossingen geïmplementeerd. Dankzij jarenlange ervaring en hooggekwalificeerde kennis van organisaties, oplossingen en technologieën, kan Traxion u ondersteunen op strategisch, tactisch en operationeel niveau als de System Integrator voor uw Identity Management oplossing.

Traxion onderhoudt nauwe contacten met de belangrijkste leveranciers op het Identity & Access Management vakgebied. Op deze manier blijven we op de hoogte van de laatste ontwikkelingen en hebben we toegang tot directe ondersteuning en detail product informatie.

Waar staat Shibboleth voor?

Het woord Shibboleth komt uit het Hebreeuws wat letterlijk “aar van graan” of “stortvloed van water” betekent. Het gebruik van het woord Shibboleth wordt in de Hebreeuwse bijbel beschreven in Judas 12:5-6. Het verhaal, in de moderne vertaling, is als volgt:

"The [Gileadites](#) captured the fords of the [Jordan](#) leading to [Ephraim](#), and whenever a survivor of Ephraim said, "Let me go over," the men of Gilead asked him, "Are you an Ephraimite?" If he replied, "No," they said, "All right, say 'Shibboleth'." If he said, "Sibboleth," because he could not pronounce the word correctly, they seized him and killed him at the fords of the Jordan. Forty-two thousand Ephraimites were killed at that time."

[Bron:

<http://en.wikipedia.org/wiki/Shibboleth>]

De uitspraak van het woord Shibboleth bepaalde dus of men geautoriseerd was om de rivier Jordaan over te steken of niet.

Voor het project Shibboleth is de naam dan ook treffend gekozen. In de eigentijdse situatie moet een gebruiker voordat deze toegang krijgt tot een bepaalde

resource zich vaak authenticeren door middel van bijvoorbeeld een naam en wachtwoord. Dit is voor veel situaties ongewenst aangezien lang niet altijd de identiteit van de gebruiker bekend hoeft te zijn binnen een site, een kenmerk als type gebruiker of locatie van de gebruiker, is vaak voldoende voor autorisatie tot een bepaalde resource. Shibboleth levert de infrastructuur en technologie om dit te realiseren.

Doelgroep

De doelgroep van dit artikel is iedereen die geïnteresseerd is in Shibboleth maar niet alle detail informatie wil lezen welke op het internet te vinden is.

Leeswijzer

Uitgangspunt is dat de lezer bekend is met het jargon wat wordt gebruikt in de Identity Management markt. Veelal worden oorspronkelijke stukken tekst aangehaald zoals deze te vinden zijn op de Shibboleth site, het copyright voor deze teksten ligt bij de oorspronkelijke auteurs. Daarnaast worden voorbeeld scenario's gegeven van Shibboleth en combinaties met A-Select en gerelateerde technologieën.



Shibboleth – Wat is het?

Initiatiefnemers

Het project Shibboleth is onder andere geïnitieerd vanuit de Amerikaanse hoger onderwijs en onderzoek instellingen. Daarbij zijn onder andere partijen als NSF, IBM/Tivoli, Sun, Red IRIS, CMU, OSU, Brown en MIT aangehaakt als sponsor van geld en/of technologie en kennis.

Functie en relaties

Het project Shibboleth levert een architectuur, policy structuren, technologie en een opensource implementatie hiervan voor het delen van web resources waar autorisatie vereist is. Veelal tussen onderwijs instellingen of binnen afdelingen van deze instellingen. Shibboleth wordt gekenmerkt door de volgende concepten:

- **Federatieve administratie**
The Identity Provider (origin) campus (home to the browser user) provides attribute assertions about that user to the Service Provider (target) site. A trust fabric exists between campuses, allowing each site to identify the other speaker, and assign a trust level. Identity Provider sites are

responsible for authenticating their users, but can use any reliable means to do this.

- **Toegangscontrole gebaseerd op attributen**

Access control decisions are made using those assertions. The collection of assertions might include Identity, but many situations will not require this (eg accessing a resource licensed for use by all active members of the campus community, accessing a resource available to students in a particular course).

- **Actief privacy management**

The Identity Provider (origin) site, and the browser user, control what information is released to the Service Provider (target). A typical default is merely "member of community". Individuals can manage attribute release via a web-based user interface. Users are no longer at the mercy of the target's privacy policy.

- **Oplossingen gebaseerd op standaarden**

Shibboleth will use OpenSAML for the message and assertion formats, and

protocol bindings which is based on Security Assertion Markup Language (SAML) developed by the OASIS Security Services Technical Committee.

- **Een framework voor meerdere, schaalbare trust en policy sets (federaties)**
Shibboleth uses Federations to specify a set of parties who have agreed to a common set of policies. (A site can be in multiple Federations, though.) This moves the trust framework beyond bi-lateral agreements, while providing flexibility when different situations require different policy sets.
- **Een standaard (maar uitbreidbare) woordenlijst voor attribuutwaarden.**
Shibboleth has defined a standard set of attributes; the first set is based on the eduPerson object class that includes widely-used person attributes in higher education.

Shibboleth levert dus expliciet geen authenticatie voorzieningen en een beperkte mate van autorisatie voorzieningen. Het levert met name een transport

mechanisme voor het delen van informatie waarop sites autorisaties kunnen geven tot bepaalde resources binnen deze sites. Het werkelijk bepalen of een gebruiker geautoriseerd is gebeurt in bijna alle gevallen bij de applicatie van de Service Provider (target). Het authenticeren van een gebruiker gebeurt bij de Identity Provider (de zogenaamde origin) en kan op basis van tooling als A-Select. Daarbij is Shibboleth standaard volledig gericht op de educatieve wereld.

Voorbeeld scenario voor gebruik Shibboleth

Om de mogelijkheden van Shibboleth eenvoudiger en duidelijker uiteen te zetten is onderstaande voorbeeld scenario uitgewerkt. Het scenario speelt zich af op een universiteit welke zowel een campus als onderzoekslaboratorium bevat.

Een universiteit bestaat uit twee sites: een campus (identity provider) en een onderzoekslaboratorium, de service provider.

De campus (Identity Provider) maakt gebruik van A-Select als authenticatie voorziening. Daarnaast worden extra faciliteiten geleverd als zelf



service waarmee de gebruiker zijn eigen profiel kan beheren. Als onderliggende administratie service wordt OpenLDAP gebruikt. De campus heeft ongeveer 40.000 studenten welke alle door middel van hun studenten pas (een smartcard) zichzelf authenticeren tegen A-Select 1.5. A-Select 1.5 gebruikt hiervoor een Radius Authenticatie Service Provider die gekoppeld is aan de authenticatie software van de smartcard. De studenten loggen daarbij in zodra ze binnen het portaal van de campus komen. Ze krijgen daarbij automatisch standaard de volgende kenmerken mee: studentnummer, naam, campusstudent, emailadres

Het onderzoekslaboratorium biedt een service waarbij studenten inzage kunnen krijgen in onderzoeksresultaten van projecten welke zijn afgesloten. Het enige waarop het onderzoekslaboratorium haar gebruikers autoriseert is of de gebruiker een student is van de betreffende campus. Het onderzoekslaboratorium wil daarbij met name weten of de dienst gebruikt wordt en door hoeveel personen. Het is niet geïnteresseerd in wie de dienst gebruikt.

In bovenstaande voorbeeld biedt Shibboleth met A-Select 1.5 een werkbare combinatie. A-Select is verantwoordelijk voor de authenticatie van de gebruiker. Na authenticatie levert het een SAML assertion richting Shibboleth die vervolgens een SAML attribuut assertion richting de service provider uitgeeft. De service provider bepaalt vervolgens op basis van de aangeleverde attributen of de gebruiker geautoriseerd is. In het voorbeeld scenario verloopt e.e.a. voor de gebruiker dan als volgt:

De gebruiker logt in met zijn campus identiteit op het campus portaal en klikt vervolgens op de site van het onderzoekslaboratorium.

Op dit moment vraagt het onderzoekslaboratorium aan de identiteit provider de waarde van het attribuut "campusstudent". Doordat Shibboleth gebruikt wordt, wordt gecontroleerd of het onderzoekslaboratorium deze informatie mag hebben en gebruiken in het kader van de privacy van de gebruiker. Wanneer dit het geval is krijgt het onderzoekslaboratorium de gevraagde informatie.

Het onderzoekslaboratorium ontvangt van de identiteit

provider het gevraagde attribuut en geeft de gebruiker op basis van deze informatie toegang tot de onderzoeksresultaten.

Voor de gebruiker zijn alle onderliggende beschreven stappen transparant. De gebruiker heeft dan ook een single sign on (of enkelvoudige aanlog) ervaring en is met twee klikken op de site van het onderzoekslaboratorium en heeft toegang tot de gevraagde informatie. Voor de service provider, het onderzoekslaboratorium in het voorbeeld, is het administratie en autorisatie model zeer eenvoudig. Het hoeft geen identiteiten te onderhouden, heeft geen accounts te beheren en autoriseert op basis van slechts één attribuut, namelijk campusstudent. Simpel.

Shibboleth versus A-Select

A-Select is een authenticatie voorziening wat de volgende concepten bevat:

- Federatieve administratie
- Modulaire authenticatie voorziening

- Toegangscontrole gebaseerd op basis van attributen
- Oplossingen gebaseerd op (opensource) standaarden

Uitgaande van bovenstaande scenario kun je je afvragen wat Shibboleth nu meer levert dan A-Select? Anders gezegd, kan bovenstaand voorbeeld scenario ook met alleen A-Select worden ingevuld?

Met A-Select kan ook een federatie model worden ontwikkeld. Daarbij is het tevens mogelijk om middels SAML attribuut uitwisseling te doen. De Service Provider kan met A-Select op gelijke manier als met Shibboleth bepalen of de gebruiker geautoriseerd is.

Waarom dan Shibboleth gebruiken? Shibboleth levert als toegevoegde waarde een drietal functies:

- Actieve privacy management
- Standaard set van attribuut waardes
- Ontwikkeld voor de educatieve wereld.



Referenties

Voor dit artikel is gebruikt van de volgende bronnen:

Wikipedia – Shibboleth:

<http://en.wikipedia.org/wiki/Shibboleth>

Shibboleth Project:

<http://shibboleth.internet2.edu/>

Andere OpenSource initiatieven

Zoals in de inleiding beschreven wordt diverse OpenSource initiatieven, hoewel ze verschillende problemen oplossen, vaak in een adem genoemd. In deze context zijn OpenLDAP en OpenSAML treffend.

OpenSAML wordt gebruikt door zowel A-Select als Shibboleth voor de implementatie van het door OASIS gestandaardiseerde SAML 2.0. Het is beschikbaar als een bibliotheek van functies die samen de SAML standaard bevatten.

OpenLDAP is een LDAP versie 3 compliant directory service. De OpenLDAP directory is te gebruiken als repository voor identiteiten en autorisaties door bijvoorbeeld Shibboleth.

Met de diverse opensource initiatieven kan een federatieve identity management omgeving worden gerealiseerd inclusief identity opslag. Beheer tooling is daarbij nog relatief onderbelicht. Daarnaast zijn er ontwikkelingen gaande waarin leveranciers als SUN en Novell delen van hun Identity Management portfolio in OpenSource plaatsen.

Conclusie

Shibboleth levert een complete set van technologieën voor het realiseren van een federatiemodel tussen identiteit providers en service providers in een web georiënteerde wereld waar autorisatie vereist is.

Shibboleth levert ten opzichte van andere federatieve concepten (of technologieën) toegevoegde waarde in de volgende gevallen:

- wanneer de privacy van een gebruiker actief moet worden gewaarborgd, alleen procedures zijn dus niet genoeg
- wanneer de aansluitende service providers allen vallen onder de educatieve of onderzoeksinstellingen

Voor meer informatie wordt verwezen naar de genoemde referenties.