TOEGANGSBEVEILIGING VOOR WEB SERVICES

1. Beschrijving

1.1. Doelstelling

De component “Toegangsbeveiliging voor webservices” bestaat uit een aantal “libraries” die tot doel hebben om de toegang tot webservices te beveiligen. De ontwikkelaars van webservices en clienttoepassingen hoeven zich dan niet meer over de beveiligingsaspecten te bekommeren.

Concreet biedt de component de volgende functionaliteiten:

- authenticiteit van de clienttoepassing die de webservice oproept op basis van een certificaat: dit biedt ons de zekerheid over de identiteit van de clienttoepassing;
- zekerheid over de identiteit van de fysieke eindgebruiker die de oproep deed;
- garantie van de confidentialiteit door middel van encryptie via HTTPS: dit is de garantie dat de uitgewisselde berichten niet leesbaar zijn voor derden die de berichten onderscheppen;
- garantie van de integriteit: de zekerheid wordt gegeven dat de berichten onderweg niet gewijzigd worden;
- zekerheid dat de gebruiker toegang mag hebben tot de gevraagde functionaliteit.

1.2. Benadering

De oplossing bestaat uit een component aan de kant van de client (Comba client) en een component aan de kant van de server (De “Comba server”).

De “Comba client” zorgt voor de authenticiteit van de eindgebruiker en interageert daarvoor met een “assertion provider” die op basis van de credentials van de eindgebruiker een bewijs van authenticatie aflevert onder de vorm van een SAML-assertie. Deze assertie is digitaal getekend door de assertion provider.

Vervolgens stuurt de “Comba client” het bewijs van authenticatie van de eindgebruiker (SAML-assertie) samen met het eigenlijke SOAP-bericht op naar de webservice,.

Het volledige bericht wordt door de “Comba client” digitaal getekend met de private sleutel van de client toepassing.

Op basis van deze laatste handtekening authentificeert de “Comba server” de clienttoepassing. De “Comba server” verifieert eveneens de handtekening van de meegestuurde SAML-token.

Op basis van de gegevens over de eindgebruiker wordt via het User Access Management (UAM) gecontroleerd of de gebruiker toegang heeft tot de gevraagde functionaliteit of niet.

1.3. Circles of trust

In een ketting van aaneengeschakelde oproepen kan, door het principe van de circles of trust, vermeden worden dat de authenticatie van de eindgebruiker bij elke stap moet gebeuren.

Dat betekent dat, binnen een circle of trust, een webservice erop vertrouwt dat de authenticiteit van de eindgebruiker door de clienttoepassing aan het begin van de ketting correct gebeurd is.

De beschreven component ondersteunt ook het scenario waarbij de authenticiteit van de gebruiker niet gebeurt door een “assertion provider”, maar door de client toepassing zelf. In dat geval is er een sterke authenticiteit van de clienttoepassing nodig op het niveau van de webservice. De component ondersteunt een dergelijke sterke authenticiteit op basis van een toepassings- certificaat.

2. Beschikbaarheid

Het gedeelte “Comba” (cliënt en server) is beschikbaar.

De “assertion provider” is in test.

3. Gebruiksvoorwaarden herbruikbare component

De component kan door andere Belgische overheidsdiensten worden gebruikt: ja.

De gebruiksregeling moet worden afgesproken naar aanleiding van een installatieproject. Hiertoe worden de geïnteresseerde overheidsdiensten verzocht zich te richten tot uw contactpersoon.

4. Aanvraagprocedures gebruik

Richt u tot uw contactpersoon. Wij nemen het initiatief om uw vragen te beantwoorden en/of een studievergadering voor te stellen.

5. Support (servicemodus)

De supportmodaliteiten voor de diensten in productie zullen worden meegedeeld tijdens de inproductiestelling.

6. Functionele informatie

U vindt hieronder een overzicht van de door de component geboden functionaliteiten.

6.1. Beschrijving input/output van de herbruikbare component

Samengevat levert de “Comba client” volgende functionaliteiten:

- identificatie / authenticiteit van de eindgebruiker (op basis van SAML) via een “assertion provider”;
- digitaal tekenen van de SOAP-request met de private sleutel van de cliënttoepassing;
- als output wordt een SOAP-request inclusief een SAML-assertie doorgestuurd naar de webservice.

De « Comba server » biedt volgende functionaliteiten :

- de input aan de server-zijde is een digitaal getekende SOAP-request waarin een SAML-assertie vervat zit die de identiteit van de gebruiker bevat;
- controle van de digitale handtekening van de cliëntapplicatie;
- controle van de digitale handtekening van de SAML-token, afkomstig van de “assertion provider”;
- integratie met UAM voor de controle van de toegang van de gebruiker tot de gewenste functionaliteit (autorisatie).

6.2. Beschrijving van de integratie- en interfacemogelijkheden van de herbruikbare component

De “Comba client” biedt een Java-interface aan die de ontwikkelaar van de clienttoepassing kan gebruiken voor het afhandelen van de veiligheidsaspecten.

De “Comba client” interageert met de “assertion provider” via een webservice-interface om een SAML-assertie te krijgen.

De Java libraries van de “Comba server” verwerken SOAP-berichten en SAML-asserties als input.

Voor het autoriseren van de toegang van de gebruiker tot de gewenste functionaliteit wordt geïntegreerd met het UAM via een web service op basis van SAML-asserties.

Beide componenten werden getest op de applicatie servers BEA WebLogic 8.1 en IBM WebSphere 6.0. Ze zijn herbruikbaar op alle J2EE platformen. Comba-client is eveneens geschikt voor stand-alone Java toepassingen.

6.3. Beschrijving van de in aanmerking genomen volumes bij de ontwikkeling van die component

Een systeem regelt het volume aan oproepen naar de webservices.

Wanneer de webservices beschikbaar worden gesteld, moet er afgesproken worden:

- het maximum aantal requests die de cliënt per tijdseenheid kan doorsturen,
- de policy voor het blokkeren van bepaalde cliënten of groepen van cliënten, wanneer dat aantal overschreden wordt.

6.4. Beschrijving van de andere relevante elementen

De “assertion provider” levert een bewijs van authenticiteit van de gebruiker, in de vorm van een SAML-assertie.

Voor de autorisaties wordt er gebruik gemaakt van het bestaande systeem voor UAM. Hierbij verwijzen we naar de fiche met als titel “Gebruikers- en Toegangsbeheer”.

7. Technische informatie

Aan de kant van de klant bestaat de oplossing uit de Java-libraries de “Comba client”.

Aan de kant van de server bestaat de oplossing uit een J2EE security-component die interageert met de Java-libraries van De “Comba server” .

Voor het uitvoeren van de authenticiteit van de gebruikers steunt de component op de “assertion provider”. De interface van de “assertion provider” is een webservice. De uitgewisselde gegevens zijn SAML-asserties voor vraag en antwoord omtrent de authenticiteit.

Op vlak van autorisaties steunt de component op het UAM. De integratie met UAM gebeurt eveneens door het uitwisselen van SAML-asserties via een webservice.

De oplossing kan gebruikt worden op open J2EE-platformen en standaard Java-cliënt toepassingen.