SECURISATION DES ACCES POUR LES SERVICES WEB

1. Description

1.1. Objectif

Le composant « Sécurisation des accès pour les services web » consiste en une série de « libraries » destinées à sécuriser les accès aux services web. Les développeurs de services web et d'applications clientes ne doivent ainsi plus se préoccuper des aspects de sécurité.

Concrètement, ce composant offre les fonctionnalités suivantes :

- Authentification de l'application cliente qui invoque le service web sur la base d'un certificat : nous sommes ainsi sûrs de l'identité de l'application cliente ;
- Certitude quant à l'identité de l'utilisateur final qui a invoqué le service ;
- Garantie de la confidentialité au moyen d'un chiffrement via HTTPS, c'est-à-dire la garantie que les messages échangés ne peuvent être lus par les tiers qui les interceptent ;
- Garantie de l'intégrité : assurance que les messages qui circulent ne seront pas modifiés ;
- Certitude que l'utilisateur peut accéder à la fonctionnalité demandée.

1.2. Approche

La solution consiste en un composant du côté du client (« Comba client ») et un composant du côté du serveur (« Comba serveur »).

Le « Comba client » veille à l'authentification de l'utilisateur final et interagit pour ce faire avec un « assertion provider » qui, sur la base des « credentials » de l'utilisateur final, délivre une preuve d'authentification sous forme d'assertion SAML sur laquelle il appose une signature numérique.

Ensuite, le « Comba client » envoie au service web la preuve d'authentification de l'utilisateur final (assertion SAML) accompagnée du message SOAP.

Le « Comba client » appose une signature numérique sur le message complet avec la clé privée de l'application cliente.

Sur la base de cette signature, le « Comba server » authentifie l'application cliente. Le « Comba server » contrôle également la signature du token SAML.

Sur la base des données relatives à l'utilisateur final, il est vérifié via le User Access Management (UAM) si l'utilisateur a accès ou non à la fonctionnalité demandée.

1.3. Circles of trust

Grâce au principe des circles of trust, il ne faut pas chaque fois vérifier l'authentification de l'utilisateur final dans une chaîne d'invocations.

Cela signifie que, dans un circle of trust, le service web considère que l'application cliente a correctement authentifié l'utilisateur final au début de la chaîne.

Ce composant supporte également le scénario où l'authentification de l'utilisateur n'est pas l'œuvre d'un « assertion provider », mais de l'application cliente même. Dans ce cas, une authenticité élevée de l'application cliente est nécessaire au niveau du service web. Pour supporter un tel degré d'authenticité, le composant se base sur un certificat de l'application.

2. Disponibilité

La partie « Comba » (client et serveur) est disponible.

Le « assertion provider » est en phase de test.

3. Conditions d'utilisation du composant réutilisable

Le composant est utilisable par d'autres services publics belges : oui.

Les modalités d'utilisation doivent être convenues à l'occasion d'un projet d'installation. Pour ce faire, les services publics intéressés sont priés de s'adresser à la personne de contact.

4. Procédures de demande d'utilisation

Adressez-vous à la personne de contact. Nous prenons l'initiative pour répondre à vos questions et/ou proposer une réunion d'étude.

5. Support (en mode service)

Les modalités de support pour les services en production seront communiquées au cours de la mise en production.

6. Informations fonctionnelles

Vous trouverez ci-dessous un aperçu des fonctionnalités qu'offre ce composant.

6.1. Description de l'input/output du composant réutilisable

En résumé, le « Comba client » offre les fonctionnalités suivantes :

- Identification / authentification de l'utilisateur final (sur la base de SAML) via un « assertion provider » ;
- Signature numérique du SOAP-request ave la clé privée de l'application cliente ;
- En output, un SOAP-request et une assertion SAML sont envoyés au service web.

Le « Comba server » offre les fonctionnalités suivantes :

- L'input du côté du serveur est un SOAP-request revêtant une signature numérique et renfermant une assertion SAML qui contient l'identité de l'utilisateur ;
- Contrôle de la signature numérique de l'application cliente ;
- Contrôle de la signature numérique du token SAML, provenant du « assertion provider » ;
- Intégration avec le UAM pour le contrôle de l'accès de l'utilisateur à la fonctionnalité désirée (autorisation).

6.2. Description des possibilités d'intégration / d'interfaçage du composant réutilisable

Le « Comba client » offre une interface Java que le développeur de l'application cliente peut utiliser pour traiter les aspects de sécurité.

Le « Comba client » interagit avec le « assertion provider » via une interface service web pour recevoir une assertion SAML.

Les « Java libraries » du « Comba server » traitent les messages SOAP et les assertions SAML en input.

Pour l'octroi de l'accès de l'utilisateur à la fonctionnalité désirée, il est opéré une intégration avec le UAM via un service web sur la base d'assertions SAML.

Les deux composants ont été testés sur les serveurs d'applications BEA WebLogic 8.1 en IBM WebSphere 6.0 Ils sont réutilisables sur toutes les plateformes J2EE. Le Comba-client convient également aux applications Java stand-alone.

6.3. Description des éléments de volumétrie qui ont été pris en compte lors du développement de ce composant

Un système régit le volume d'invocations des services web.

Lorsque les services web sont mis à disposition, il faut déterminer :

- le nombre maximal de requests que le client peut transmettre par unité de temps,
- la policy relative au blocage de certains clients ou groupes de clients lorsque ce nombre est dépassé.

6.4. Description des autres éléments pertinents

Le « assertion provider » délivre une preuve d'authenticité de l'utilisateur sous forme d'assertion SAML.

Pour les autorisations, il est utilisé le système actuel pour le UAM. Nous vous renvoyons ici à la fiche intitulée « Gestion des utilisateurs et des accès ».

7. Informations techniques

Du côté du client, la solution consiste en les « Java libraries » du « Comba client ».

Du côté du serveur, la solution consiste en un composant de sécurité J2EE qui interagit avec les « Java libraries » du « Comba server ».

Pour l'authentification des utilisateurs, le composant repose sur le « assertion provider ». L'interface avec le « assertion provider » est un service web. Les données échangées sont des assertions SAML pour question et réponse concernant l'authenticité.

Au niveau des autorisations, le composant repose sur le UAM. L'intégration avec le UAM s'opère également par l'échange d'assertions SAML via un service web.

La solution peut être utilisée sur des plateformes J2EE et des applications clientes Java standard.