Fédération des identités (SAML 2, OpenID Connect), synthèse

Cours Synthèse de 2 jours - 14h
Réf : FED - Prix 2025 : 1 990 HT

Ce cours de synthèse présente les cas d'usages, la sémantique et les architectures logicielles associés à l'implémentation des standards SAML 2 / OAUTH 2.0/OpenID Connect dans le cadre d'un projet lié à l'utilisation des identités distantes, avec les outils du commerce et l'interaction avec les technologies existantes.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Connaître les services et cas d'usage de SAML 2

Maîtriser la syntaxe et sémantique de SAML 2

Connaître les technologies associées à SAML 2

Intégrer OAUTH 2.0/OpenID Connect au SI

Intégrer SAML 2 au SI

LE PROGRAMME

dernière mise à jour : 05/2024

1) Les cas d'usage

- SAML 2 : les services qu'il peut rendre, MDSSO, Fédération d'identité, Web Service.
- Les différents acteurs impliqués : DSI, architectes, développeurs, exploitants.
- Liaison et fédération d'identités : choix des services, du type d'identifiant et de la dynamique de fédération.
- Fournisseur d'identité : Web SSO en IDP (Identity Provider) Initiated SSO ou OP OpenID Connect.
- Fournisseur de service : le SP (Service Provider) SAML V2 ou le RP (Relaying Party) OpenID Connect.
- Web Browser SSO : les étapes d'authentification d'un utilisateur et les aller-retour entre le Client et le Serveur.
- SAML 2 et les Web Services : utilisation des assertions. Assertions SAML 2 et Secure Token Service (STS).
- Oauth 2.0 et l'Access Token. OpenID Connect et l'Id Token.

2) SAML 2

- La syntaxe et les concepts : SOAP/XML, assertions, protocols, binding, profile, authentification context, metadata.
- Les "Bindings" : HTTP Redirect, HTTP Post, HTTP Artifact, SAML SOAP, Reverse SOAP, SAML URI.
- Profils définis dans SAML 2.0 : Web Browser SSO, ECP, IDP Discovery, Single Logout, Assertion Query/Request.

3) OAUTH 2.0

- La syntaxe et les concepts : REST, Autorisation, Scope, Access Token, Refresh Token.
- Les acteurs et leurs rôles.
- Les scénario : Code , Implicit, Client Credentials, Password.

PARTICIPANTS

Ce cours s'adresse aux responsables réseaux, architectes, responsables études, ingénieurs système et développeurs qui ont à intégrer une solution utilisant SAML 2.

PRÉREQUIS

Connaissances de base des architectures techniques Web.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

4) OpenID Connect

- La syntaxe et les concepts : REST, Json, JWT, ID_Token.
- Les acteurs et leurs rôles.
- Les scénarios : Code, Implicit, Hybrid Flow.

5) Etude de cas d'intégration au système d'information

- 1 : Utilisation SAML V2 - Création d'un IDP SAML V2.
- 2 : Utilisation SAML V2 - Création d'un SP SAML V2.
- 3 : Utilisation OpenID Connect - Création d'un OP OIDC.
- 4 : Utilisation Oauth 2.0 et OpenID Connect - Avec ADFS ou Keycloak.
- 5 : Utilisation OpenID Connect - France Connect.

6) SAML 2 et OAUTH 2.0/OpenID Connect

- Les produits et module OpenSource (simplesamlPHP, Shibboleth, mod_auth_mellon,mod_auth_openidc).
- Les produits commerciaux (IBM,Microsoft,Oracle, CA, Forgerock,...).
- Comparaison des services et interopérabilité.

Démonstration : Présentation et démonstration de certains produits.

7) SAML 2 et OAUTH/OpenID Connect et les autres technologies

- SAML 2 , Oauth 2.0/OpenID Connect et Kerberos.
- PKI, WS-Federation et OpenIDConnect.

LES DATES

CLASSE À DISTANCE
2025 : 23 sept., 09 déc.