Gestion des identités & sécurité des accès

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Management du SI

Filière : Séminaires décideurs

Rubrique : Enjeux du SI

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

Identifier les enjeux de la gestion d'identité Déterminer les apports de la gestion d'identité à partir d'un SI centralisé : la sécurité d'accès aux applications, la modélisation des processus, la valorisation du portail d'entreprise et l'ouverture de son SI par la fédération d'identité

Public visé

Architecte Direction du SI
Direction informatique
Maîtrise d'ouvrage
Responsable études Urbaniste

Pré-requis

Notions d'annuaire et XML. Être sensibilisé à la sécurité du SI et aux Web services.

PROGRAMME

1. **LA GESTION DES RÉFÉRENTIELS D'IDENTITÉS**
Introduction .
Constat d'hétérogénéité du SI. .
Centralisation de l'information. .
Gestion à partir d'un point d'accès unique. .
Présentation des annuaires LDAP. Les outils .
Synchronisation des référentiels par le provisioning. .
Agrégation des données par le dé-provisioning. .
Le méta-annuaire ou l'annuaire virtuel ? .
Présentation des outils évolués de gestion de contenu d'annuaire.
Les DCMS. La gestion des habilitations . L'information pertinente. .
Les modèles de données RBAC et ORBAC.

2. LA SÉCURISATION DES ACCÈS
Renforcer la politique de mots de passe.
L'unification des mots de passe.
Le modèle actuel de sécurisation des accès : la signature unique.
Présentation des architectures de Web SSO.
Étude de scénarios Web SSO.
Présentation de solutions de Web SSO.
Étude de solutions Open Source.
La limitation du Web SSO est couverte par l'Entreprise SSO.

3. L'AUTHENTIFICATION FORTE
Cryptographie.
Les bases de la cryptographie.
Les algorithmes à clé secrète, clé publique, hachage, signature électronique. .
Répondre aux fondamentaux de la sécurité : authentification, confidentialité, intégrité, non répudiation et disponibilité. Fonctionnement des PKI.

Code de formation : S-IAM

IAM, ANNUAIRE, LDAP, RBAC, ORBAC, PROVISIONING, DCMS, SÉCURITÉ, SSO, AUTHENTIFICATION, CRYPTOGRAPHIE, PKI, XPDL, PROCESSUS, BPM, WORKFLOW, WEBSERVICES, FÉDÉRATION, SAML

€ Tarifs

Prix public : 1420 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 14 heures

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

Informations non contractuelles - PDF généré le 28/11/2026

Les infrastructures à clé publique.
Environnements de confiance.
Autorités de certification.
Certificats X509 : types classe et fonctionnement.
Les Processus métier
Études de cas pratique.
Embauche d'un nouveau salarié.

Exception à une règle de sécurité.
Définitions.
Le BPM vs workflow vs processus.
Activité, transition, participant.
La coalition Wfmc.
Le Format Xpdl.
Présentation du protocole Asap et de la spécification Wfxml.
Les outils.
Modélisation de processus.
Interaction avec le processus.
Suivi et console de pilotage.
Sécurisation des Web services
Sécurisation des messages Xml.
Xml-Signature : signature des messages.
Xml-Encryption : chiffrement des messages.
Ws-Security : normalisation de la sécurisation des messages.
Interaction avec les PKI.
Xkms : gestion du cycle ce vie des certificats.
Délégation d'authentification et gestion de droits.
Saml, Ws-Federation : échange des informations d'authentification.
Xacml, Ws-Authorization : échange des informations d'autorisation.
Provisioning. Spml : gestion des comptes utilisateur.
La fédération d'identité.
Fonctionnement des serveurs d'identité.
Le projet Liberty Alliance.
Le projet Cardspace.
Le projet Openid.
Le projet Shibboleth.
Le projet Concordia.

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.

Informations non contractuelles - PDF généré le 28/11/2026