

Gestion des identités et sécurité des accès

4 jours (28 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

3 500 € HT par personne (TVA en vigueur) **Repas inclus en présentiel**

Contenu mis à jour le 25/09/2026. Document téléchargé le 07/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Renforcer la sécurité et simplifier l'accès aux informations pour les organisations
- Etendre le Single Sign-On (SSO)
- Intégrer une Public Key Infrastructure (PKI)
- Evaluer les services Cloud sur l'authentification à l'intérieur d'un système d'information (SI)
- Mettre en oeuvre un système de fédération.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Ingénieurs système, ingénieurs en sécurité, administrateurs système, chefs de projets en sécurité, MOE (maîtres d'oeuvre) et/ou MOA (maîtres d'ouvrage).

Prérequis

Avoir des connaissances de base sur la sécurité des systèmes d'information et une bonne maîtrise des systèmes et des infrastructures.

Programme

1 Pendant votre formation

Gestion des identités et sécurité des accès

Jour 1

Etat de l'art de l'IAM (Identity and Access Management)

- Constat d'hétérogénéité du SI
- Centralisation de l'information
- Rôle de la PSSI dans la mise en place d'un IAM
- Environnement normatif et réglementaire
- IAM dans le contexte de souveraineté
- Gestion à partir d'un point d'accès unique
- L'annuaire centralisé vs l'approche fédérative
- L'administration et la gouvernance des identités
- L'autorisation
- Le critère CIDT
- Les trois états de la donnée
- Caractérisation de la sensibilité de l'information
- Les protocoles d'authentification
- Les bases de données d'authentification

Exemples de travaux pratiques (à titre indicatif)

- *Présentation de l'étude de cas*
- *Présentation des documents nécessaires à la mise en place d'un IAM*
- *Fourniture des documents afférents*
- *Discussion générale sur l'étude de cas*

Jour 2

Implémentation d'une systémique cryptographique

- Petite histoire du chiffrement
- Le besoin de confidentialité
- La signature numérique
- Le chiffrement
 - Symétrique
 - Asymétrique
- Notion de certificats
- Les PKI et les certificats

- Evaluer les relations de confiance avec les CA (Certificate Authorities) externes
- Contrôler l'accès avec les certificats d'attributs
- Elaborer une stratégie de gestion des certificats
- Sécurisation des clés privées
- Utiliser un agent de récupération des clés
- Associer des identités à des certificats
- Gestion de la révocation des certificats

Exemples de travaux pratiques (à titre indicatif)

- *Création et manipulation de certificat (chiffrement et signature)*
- *Mise en place de la PKI concernant l'étude de cas*

Jour 3

Fédérer des identités

- Authentification locale, accès distant
- Garantir l'interopérabilité et la portabilité des identités
- Notion d'ISP et IDP
- Présentation
 - De "France Connect" et services équivalents
 - Des protocoles d'échange SAML, OAuth et OpenID Connect
 - Des protocoles d'origine OASIS
- Partage des identités avec le Cloud
- Décorrélation des ressources et des services
- Organisation de la gestion des identités (RBAC-ABAC-...)
- Présentation d'Azure pour les applications SaaS
- Fédération Amazon AWS
- S'authentifier avec les rôles IAM d'Amazon

Exemples de travaux pratiques (à titre indicatif)

- *Présentation de keycloak*
- *Installation de keycloak dans le cadre de l'étude de cas*
- *Mise en place du portail SSO*

Jour 4

Gestion des identités pour les appareils mobiles

- Les problèmes nouveaux
 - Les smartphones et tablettes
 - Le mode déconnecté pour les mobiles avec bases de données intégrées
- Notion de BYOD (Bring Your Own Device) et ses conséquences
- La restriction des périmètres fonctionnels

- Notion BYOID (Bring Your Own IDentity) : "Apportez votre identité"
- Contrôle des coûts d'implémentation
- Réduire le coût total de possession
- Zero Trust : la solution idéale pour réduire l'exposition
- AWS, Azure, Microsoft et les solutions pour le BYOD
- Conclusion et perspective

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 11 mai 2027 au 14 mai 2027 (4 jours / 28 heures)

Aix-en-Provence

Du 11 mai 2027 au 14 mai 2027

Aix-en-Provence

- 11 mai 2027 9h00 – 15h30
- 12 mai 2027 9h00 – 15h30
- 13 mai 2027 9h00 – 15h30
- 14 mai 2027 9h00 – 15h30