

# Formation Keycloak : sécuriser et intégrer l'authentification dans vos applications

Réf. SF34513

Déléguez l'authentification et l'autorisation de vos applications web, mobiles et de vos API à Keycloak, avec les flux et les bonnes pratiques de sécurité qui font référence.

|              |                                   |                                  |                       |
|--------------|-----------------------------------|----------------------------------|-----------------------|
| 3 j<br>Durée | 2 100 € HT<br>Inter / participant | 10 000 € HT<br>Intra (≤12 pers.) | 0<br>Sessions à venir |
|--------------|-----------------------------------|----------------------------------|-----------------------|

## Objectifs pédagogiques

- ✓ Configurer un realm et des clients Keycloak adaptés à chaque type d'application
- ✓ Implémenter les flux OAuth 2.0 et OpenID Connect recommandés selon le contexte applicatif
- ✓ Sécuriser une application web, une SPA et une API REST avec les bibliothèques OpenID Connect standard
- ✓ Mettre en œuvre des stratégies d'autorisation par rôles, groupes, scopes et politiques centralisées
- ✓ Adapter les parcours d'authentification côté application : fournisseurs externes, authentification renforcée, personnalisation
- ✓ Intégrer Keycloak au cycle de développement : environnement reproductible, tests et sécurité des jetons

## Public visé & prérequis

**Public visé** Architectes logiciens, Développeurs, Ingénieurs DevOps

**Prérequis**- Bonne pratique du développement web côté serveur (Java, JavaScript, Python ou autre) et notions de développement frontend - Familiarité avec les API REST, HTTP et JSON - Notions de TLS et de sécurité applicative - Aisance avec la ligne de commande et les conteneurs (l'environnement de travail est conteneurisé)

## Programme détaillé

### Fondamentaux de Keycloak pour les développeurs

- Gestion des identités et des accès : ce que l'application délègue au fournisseur d'identité et ce qu'elle garde
- Modèle de Keycloak : realms, clients, utilisateurs, rôles, groupes et client scopes
- Console d'administration : les écrans utiles au développeur au quotidien
- Environnement de développement : instance conteneurisée locale et realm prêt à l'emploi
- Endpoints exposés par un realm : discovery, autorisation, jeton, informations utilisateur, déconnexion

#### Activités pratiques :

- Démarrage d'une instance locale, création d'un realm et d'un premier client, test du cycle connexion/déconnexion
- Exploration du discovery endpoint et des métadonnées d'un realm

### OAuth 2.0 et OpenID Connect en pratique

- OAuth 2.0 : acteurs, rôles et principe de la délégation d'autorisation
- OpenID Connect : couche d'identité, jeton d'identité et informations utilisateur
- Jetons JWT : structure, claims, signature et durée de validité
- Authorization Code avec PKCE : le flux de référence pour les applications avec utilisateur
- Client Credentials et Device Authorization : échanges entre services et appareils à saisie limitée
- Rafraîchissement, révocation et déconnexion : cycle de vie complet d'une session
- Flux hérités (Implicit, Resource Owner Password) : pourquoi ils sont écartés aujourd'hui

#### Activités pratiques :

- Décodage et inspection de jetons d'accès, d'identité et de rafraîchissement

- Mise en œuvre pas à pas d'un Authorization Code avec PKCE, puis d'un échange Client Credentials

## Sécuriser les applications web et les SPA

- Clients publics et confidentiels : choisir le bon type selon l'application
- Paramétrage du client : URI de redirection, Web Origins, secrets et rotation
- Bibliothèques OpenID Connect des frameworks : intégration côté serveur (Java, JavaScript, Python... selon le contexte des participants)
- Applications monopage : stockage des jetons dans le navigateur, risques associés et pattern backend-for-frontend
- Sécurisation sans modification du code : délégation de l'authentification à un reverse proxy
- Sessions et déconnexion : session applicative, session SSO, déconnexion propagée

### Activités pratiques :

- Sécurisation d'une application web côté serveur avec la bibliothèque OIDC de son framework
- Connexion d'une application monopage et comparaison des stratégies de stockage des jetons
- Protection d'une application existante par reverse proxy, sans toucher au code

## Sécuriser les API, les services et les applications mobiles

- API en resource server : où et quoi vérifier avant d'accepter une requête
- Validation des jetons : signature via les clés publiques du realm (JWKS) ou introspection auprès du serveur
- Contrôles indispensables : émetteur, audience, expiration, scopes et rôles attendus
- Microservices : propagation de l'identité et de l'autorisation entre services
- Machine-to-machine : comptes de service et clients confidentiels
- Applications mobiles et natives : Authorization Code avec PKCE, navigateur système et stockage sécurisé des jetons

### Activités pratiques :

- Sécurisation d'une API REST avec validation locale des jetons et contrôle de l'audience
- Appel d'une API par un service technique via un compte de service
- Chaînage de deux services avec propagation du contexte d'authentification

## Stratégies d'autorisation

- Rôles de realm, rôles de client et rôles composites : structurer les droits d'une application
- Groupes et héritage des droits : RBAC et GBAC en pratique
- Scopes OAuth 2.0 : restreindre ce qu'une application peut demander
- Protocol mappers : claims personnalisés, attributs utilisateurs et audiences dans les jetons
- Authorization Services : ressources, politiques et permissions gérées côté Keycloak
- Choisir son modèle : autorisation portée par les jetons ou déléguée au serveur, avantages et limites
- Gestion déléguée des autorisations par l'utilisateur (UMA) : principe et cas d'usage

### Activités pratiques :

- Contrôle d'accès par rôles et par groupes dans une API
- Ajout de claims personnalisés dans un jeton et exploitation côté application
- Mise en place de politiques et de permissions avec Authorization Services

## Parcours d'authentification et fédération vus de l'application

- Fournisseurs d'identité externes : ce que l'application voit d'un brokering (Microsoft Entra ID, autre Keycloak, fournisseurs sociaux)
- Sélection d'un fournisseur depuis l'application et liaison avec un compte existant
- Claims issus du fournisseur externe : récupération, transformation et usage applicatif
- Authentification renforcée à la demande : exiger un second facteur sur une opération sensible
- Actions requises et enrôlement : compléter un profil, vérifier un e-mail, activer un facteur
- Personnalisation du parcours : habillage des pages de connexion et des e-mails
- Extension du serveur par SPI : ce qu'il est possible de développer, et quand cela se justifie

### Activités pratiques :

- Ajout d'un fournisseur d'identité externe et exploitation des informations reçues dans l'application
- Déclenchement d'une authentification renforcée sur une action sensible d'une application

## Industrialisation et bonnes pratiques

- Realm de développement reproductible : export, import et démarrage automatisé de l'environnement
- Tests : instance Keycloak jetable pour les tests d'intégration d'une application sécurisée
- Configuration par environnement : secrets clients, URL de redirection, séparation développement/production
- Admin REST API : les besoins applicatifs légitimes (création de comptes, actions sur les utilisateurs) et leurs limites
- Bonnes pratiques de sécurité des jetons : durées de vie, stockage, rotation, journalisation
- Checklist avant mise en production et passage de relais aux équipes d'exploitation

**Activités pratiques :**

- Mise en place d'un realm importé automatiquement au démarrage de l'environnement de développement
- Écriture d'un test d'intégration d'une API sécurisée sur une instance Keycloak jetable

## Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans  
d'expertise

1 068+  
formations

11 178  
apprenants formés/an

+67  
Net Promoter Score

### Avis des participants

**Note moyenne des participants de la filière Cybersécurité et Protection des Données : 4,9/5 — 13 avis**

**William B.** — Prévoir l'envoi à chaque participant du livre de CISS au moins un mois avant la formation.

**Mickael L.** — il est top Romain GARCIA

### Ils nous font confiance

Cette année notre filière Sécurité Applicative (AppSec) a accompagné plus de 14 entreprises dont :

ACTIMAGE CONSULTING SAS AIGA ALCYOR ALDORIA BPO FOUR JS DEVELOPMENT TOOLS GIE AG2R GROUPE FDJ IT LINK FRANCE REGION HAUTS DE FRANCE +4 autres

### Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



### Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

**0 805 950 800**

[demande@sparks-formation.com](mailto:demande@sparks-formation.com)