Mobile ID OpenID Connect

Une authentification sécurisée et renforcée – totalement intégrée au flux d'utilisateurs

Les nouveaux systèmes de licence et de déploiement (SaaS) permettent de créer des systèmes distribués avec de nouvelles exigences en termes de solutions IAM et MFA. Mobile ID OpenID Connect (OIDC) permet des scénarios d'utilisation très variés en liaison avec des systèmes fédérés. Il permet une utilisation et une distribution aisées de Mobile ID grâce à l'indication des points de terminaison techniques auprès de votre fournisseur d'identité (FdI).

Swisscom garantit que tous les utilisateurs, quelle que soit leur situation initiale, puissent procéder à une authentification renforcée. Si Mobile ID n'est pas encore installé et activé, les utilisateurs seront guidés par le processus d'activation. Vos utilisateurs voient toujours une authentification complète. Diverses données supplémentaires, par ex. le lieu de l'utilisateur, peuvent également être ajoutées au titre de services en option.

La seule condition pour pouvoir utiliser Mobile ID OIDC est que vos utilisateurs possèdent un téléphone portable et puissent recevoir des SMS. Mobile ID fonctionne dans le monde entier. Posséder une carte SIM Swisscom ou l'installation de l'appli Mobile ID est indispensable pour la détermination des données de position.

Les avantages offerts par Mobile ID OIDC

Intégration facile

Configuration facile des points de terminaison indiqués avec FdI. ✓

Guidage de l'utilisateur par Swisscom

Processus entièrement basé sur le Web pour vos utilisateurs. ✓

Idéal pour les environnements hybrides

Coexistence avec d'autres intégrations Mobile ID. ✓

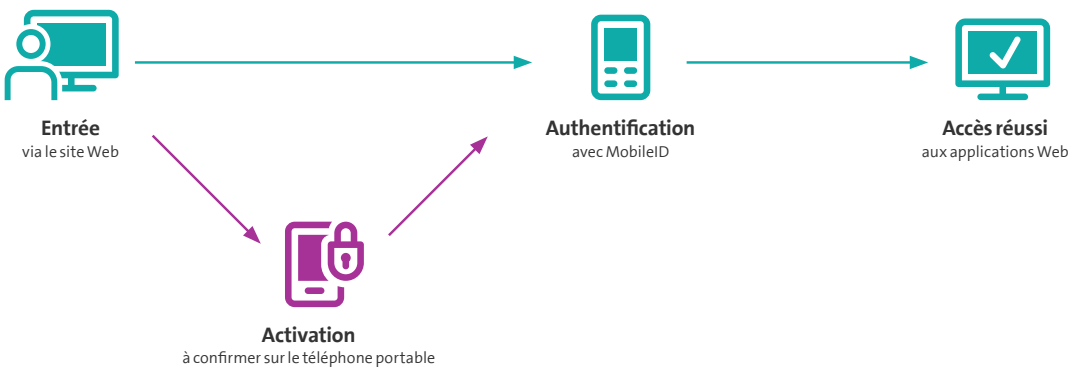
Compatibilité cloud

Par exemple pour Microsoft Azure MFA, Microsoft Active Directory et AWS. ✓

Services et prestations supplémentaires en option

Possibilités d'extensions personnalisées et répondant aux besoins spécifiques des clients. ✓

Voici comment fonctionne Mobile ID OpenID Connect



swisscom

Présentation de Mobile ID OpenID Connect

Que propose le pack de base?
Quelques explications à propos des services de base de Swisscom Mobile ID OpenID Connect.

Services de base

- **Utilisation comme deuxième facteur:** Authenticator permettant de compléter facilement les authentifications existantes pour tous les détenteurs d'un téléphone mobile.
- **Moyen d'authentification Mobile ID:** Authentification renforcée basée sur SIM/appli via «Possession et savoir/inhérence». Disponible en Suisse, dans l'UE et d'autres pays.
- **Interface Mobile ID Open ID Connect:** Prise en charge simple des applications Web dans les systèmes fédérés (FdI) en référençant les points de terminaison du service ID OIDC.
- **Garantir le niveau de protection défini:** Les processus de distribution, d'activation et de remplacement Mobile ID résolvent les problèmes typiques des jetons matériels et permettent de garantir une authentification sécurisée à tout moment via «Savoir et possession».
- **Pseudonyme unique et non modifiable:** Le «sub» permet de garantir en tout temps qu'il s'agit des mêmes utilisateurs précédemment enregistrés.
- **Authentification OIDC standardisée:** Les scopes «openid» et «profile» permettent d'avoir accès au OpenID Connect Provider (OP) développé par Swisscom.
- **Mobile ID et Microsoft Azure AD:** Configurations développées par Microsoft pour l'utilisation de Mobile ID avec Azure AD B2C.

Nous vous proposons les services supplémentaires suivants:
Les extensions Swisscom Mobile ID OIDC répondant à vos besoins.

Services en option

- **Informations complémentaires:** Les scopes «phone», «mid_profile», «mid_cms» et «mid_location» offrent une sécurité supplémentaire et permettent d'obtenir plus d'informations.
- **Pseudonyme pour la reconnaissance:** Reconnaître une personne via plusieurs inscriptions/connexions et instances d'application.
- **Authentification renforcée:** En étant en possession d'un matériel informatique spécifique et d'un élément de sécurité supplémentaire correspondant (AL3).
- **Identification personnalisée de l'utilisateur:** Authentification renforcée et garantie d'être en possession d'un certificat (AL4).
- **Texte personnalisé:** Les clients peuvent modifier et/ou compléter les textes d'authentification à leur guise.
- **Mobile ID Zero Trust:** Toutes les confirmations sont basées sur une cryptographie puissante. Elles peuvent être vérifiées par le client et attribuées au propriétaire concerné de Mobile ID de manière inviolable.
- **Authentification consécutive:** Les données d'utilisateurs actuelles peuvent être comparées à plusieurs reprises.
- **Utilisation et facturation simultanées:** Via le contrat Mobile ID existant (API REST).

Services supplémentaires: Des mises en page spécifiques aux clients peuvent être utilisés pendant les processus d'authentification. Par ailleurs, les processus et contenus de l'authentification sont modifiés pour répondre aux besoins spécifiques des clients. La migration des «jetons» existants, par ex. Authenticator ou RSA, sera faite à l'aide du processus standardisé. Nos services de consultation propose des conseils spécialisés au sujet d'IAM, de la sécurité et la continuité d'activité.

Swisscom (Suisse) SA Clients Commerciaux, case postale, CH-3050 Berne
Téléphone 0800 800 900, www.swisscom.ch/enterprise