

OPENOTP SECURITY SUITE

SOLUTION D'ENTREPRISE
DE MFA & IAM TOUT-EN-UN

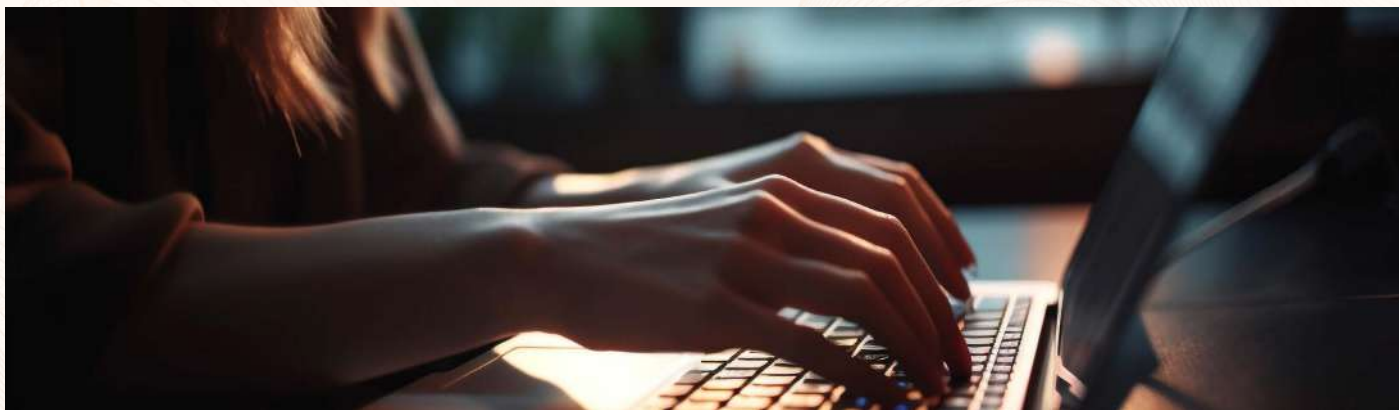


LA SOLUTION DE MFA LA PLUS COMPLÈTE À CE JOUR

OpenOTP Security Suite est bien plus qu'un simple serveur d'authentification multifacteur. C'est le couteau suisse de l'authentification, offrant un large éventail de méthodes 2FA et une vaste gamme d'API, s'intégrant à toute application ou service d'entreprise, qu'il soit hébergé dans le cloud ou on-premise.

NOTRE ENTREPRISE

Éditeur européen spécialisé dans la gestion des identités et des accès (IAM) et l'authentification multi-facteurs (MFA), RCDevs Security propose des solutions de sécurité modulaires et flexibles, disponibles en mode on-premise ou SaaS. Reconnue pour la fiabilité de ses logiciels et un haut niveau de satisfaction client, RCDevs accompagne aussi bien les PME que les grandes entreprises, tous secteurs confondus, à travers le monde.



LA FORCE DE LA PLATEFORME WEBADM

Bien plus qu'un simple serveur MFA, OpenOTP Security Suite est une plateforme IAM modulaire pilotée par WebADM alliant gestion centralisée des identités et flexibilité.

Gestion centralisée et unifiée

WebADM centralise la gestion des **identités locales et cloud** (Active Directory, OpenLDAP, Entra ID, Google Workspace...) pour une administration unifiée, même en environnement hybride.

Contrôle d'accès avancé

Son **interface d'administration** permet de définir des politiques d'accès avancées par système, utilisateur ou groupe, pour un contrôle précis et personnalisé de la sécurité.

Une solution évolutive

La suite OpenOTP combine puissance, simplicité et agilité pour une **gestion des accès** qui suit le rythme de votre entreprise.

CARACTÉRISTIQUES & AVANTAGES

Sources d'identités multiples

→ Parfait pour les **environnements hybrides** combinant plusieurs annuaires locaux (LDAP/AD) et **services d'identité cloud** (Entra ID, Duo, Okta, Ping Identity etc.).

Haute disponibilité

→ **Clustering actif-actif** pour garantir une disponibilité continue des services et faciliter les mises à jour.

Gestion d'identité

→ Les **identités LDAP et cloud** sont gérable via les interfaces web ou API.

Redondance

→ Redondance et bascule automatique assurent la disponibilité des services essentiels.

Architecture modulaire

→ Solution évolutive permettant d'étendre facilement ses capacités et fonctionnalités.

HSM

→ Prend en charge l'utilisation de **modules de sécurité matérielle** (HSM) pour chiffrer des données confidentielles telles que les clés des tokens.

COMMENT ÇA FONCTIONNE

OpenOTP Security Suite s'intègre facilement à votre infrastructure existante et déploie la sécurité multifacteur sans complexité.



Connexion native aux identités

OpenOTP interagit en temps réel avec vos sources d'identité, **locales ou cloud** grâce à des connecteurs assurant une intégration simple et continue.



Politiques d'accès centralisées

Définissez des règles précises selon les utilisateurs, groupes et contextes (IP, horaires, géolocalisation...). L'authentification s'adapte au niveau de risque.



Méthodes d'authentification flexibles

OTP, push mobile, FIDO2, Passkeys, SMS, e-mail, Smartcard, Magic Links... Choisissez **les méthodes les plus adaptées** à vos besoins.



Intégration transparente

OpenOTP supporte de nombreuses intégrations via des plugins, APIs et standards (RADIUS, LDAP, SAML2, OIDC & OAuth2).



Expérience utilisateur fluide

L'utilisateur s'authentifie rapidement via un **second facteur simple**, pour une sécurité renforcée et une adoption facilitée.

MÉTHODES D'AUTHENTIFICATION



OpenOTP Token App

Push mobile
ou OTP token



PKI

Authentification basée
sur le certificat utilisateur



Magic Links

QRCode par Mail ou SMS
pour confirmer l'accès



YubiKey

YubiOTP, OATH-HOTP
& PIV



FIDO2

Authentification par
cryptographie à clé publique



Tokens Logiciels

OATH basé sur
l'événement et le temps



Tokens Physiques

OATH basé sur
l'événement et le temps



Méthodes Traditionnelles

OTP par SMS, par Mail & Mail
sécurisé ou liste imprimée

APPLICATIONS ET SERVICES TIERS

RADIUS universel

Protégez l'accès à vos VPN
et équipements réseau (Citrix,
Cisco, Pulse Secure, F5,...)

Sécurisation des authentifications LDAP

Le proxy LDAP permet d'ajouter
la MFA à toute application
supportant le protocole LDAP.

Services compatibles ADFS

Prise en charge de la MFA pour
toutes les authentifications via
ADFS, incluant Outlook Web
Access, Office 365, SharePoint...

Fédération d'identité & SSO

Support d'OpenID Connect,
OAuth 2.0 et SAML2 pour
une authentification fédérée
sécurisée avec Single Sign-On.

Sessions MacOS

Renforcez l'ouverture de session
macOS avec une authentification
multifactor intégrée.

Environnement Windows

Sécurisez RDS et postes Windows
avec une MFA flexible, adaptée
aux environnements complexes.

Réseaux Wi-Fi & filaires

Sécurisez l'accès à vos réseaux
grâce à une authentification forte
basée sur les protocoles EAP-TLS
et EAP-TTLS

Environnements Unix/Linux

Ajoutez la MFA à tous
vos services Linux/UNIX
s'appuyant sur les mécanismes
d'authentification PAM

Authentification hors ligne

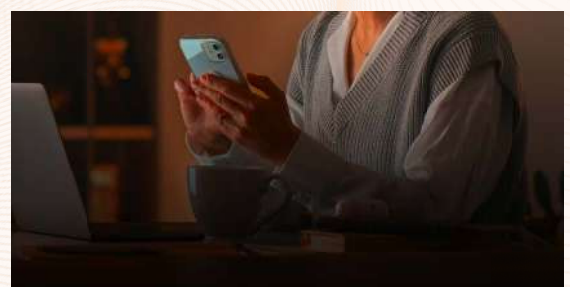
Support de la MFA en mode
déconnecté sur Windows
et macOS, via clés FIDO2 ou
application OpenOTP Token.

APIs

Intégrations personnalisées,
automatisables et optimisées
pour les environnements DevOps.

Librairie

Bibliothèques de développement
disponibles pour C, C++, PHP,
Python, .NET...



APPLICATION TOKEN OFFICIELLE

Notre application gratuite **OpenOTP Token** propose
des notifications Push sous diverses formes, en
complément des OTP traditionnels. Elle intègre
également des fonctionnalités avancées telles que
le **badging OpenOTP**, l'alerte en cas de tentative
de hameçonnage, le géomapping, la **protection
biométrique**, ainsi que la signature électronique.



MODES DE DÉPLOIEMENT

RCDevs s'adapte à tous vos besoins d'infrastructure grâce à ses multiples options de déploiement, vous offrant souplesse, sécurité et performance.

On-Premise

Déployez la solution localement sur **serveurs physiques, virtuels ou conteneurs Docker**. RCDevs propose également des repositories Debian/RPM et des appliances prêtes à l'emploi.

Cloud privé dédié

Hébergé par RCDevs sur une infrastructure dédiée ou installé sur votre cloud privé existant.

SaaS hébergé

Solution **clé en main** hébergée et gérée par nos équipes, accessible immédiatement sans installation.



SIGNATURE ÉLECTRONIQUE

Support multi-niveaux

Signatures électroniques simples, avancées et qualifiées conformes aux exigences réglementaires.

Contrats liés à l'accès

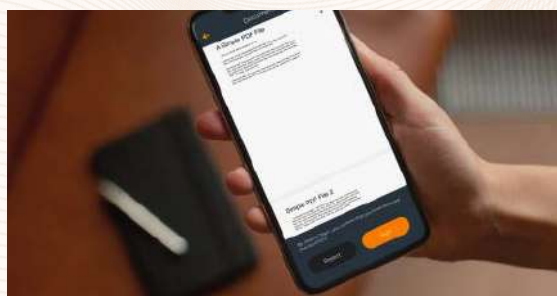
L'accès aux systèmes est bloqué tant qu'un document (ex : NDA) n'a pas été signé électroniquement. Le workflow de signature avec l'utilisateur est entièrement automatisé.

Intégrations prêtes à l'emploi

Plugins disponibles pour **Nextcloud**, **Postfix** (déclenchement de signature via email avec pièce jointe), et **Windows** (signature instantanée par clic droit sur un document).

API ouvertes

Intégrez facilement la signature électronique dans vos applications tierces via nos API.



SELF-SERVICES INCLUS

Administration Help-Desk

Application web intuitive offrant une **interface simple** pour le support informatique de premier niveau et la gestion quotidienne des opérations avec vos utilisateurs.

User Self-Service Desk

Permet aux utilisateurs de gérer l'enrôlement de leurs tokens, **clés FIDO/Passkeys** certificats, méthodes d'authentification et opérations de badging.

Secure Password Reset

Application web en libre accès ou accessible sur demande, permettant aux utilisateurs de réinitialiser leur mot de passe AD, LDAP, Entra ID, etc.

User Self-Registration

Simplifiez et automatisez l'enrôlement des utilisateurs grâce à l'envoi de **liens uniques sécurisés** offrant un accès immédiat au portail d'enrôlement.



BADGING

Garantissez un accès sécurisé à vos systèmes d'entreprise grâce à une gestion fine basée sur la localisation de vos utilisateurs et les zones ou pays autorisés.

Rotation automatique des mots de passe

Les mots de passe utilisateurs sont renouvelés automatiquement à chaque opération de **badging**, renforçant la sécurité.

Compte verrouillé par défaut

Le compte utilisateur reste inutilisable tant que l'accès n'a pas été explicitement demandé via le badging.

Politiques d'accès personnalisées

L'accès à un système peut être conditionné à un badging préalable, que ce soit **depuis un device mobile ou via le portail self-service**.

Badging automatisé

L'opération se déclenche automatiquement lorsque le device et l'authentification réseau (Wi-Fi ou filaire) sont intégrés au **système NAC** de RCDevs.