Le serveur IDCONFIRM 1000

Grâce à des solutions plug-and-play adaptables aux réseaux existants, aux serveurs AAA et étant fabriquées selon les normes OATH, la plate-forme IDConfirm comprend tous les composants nécessaires au déploiement de l'authentification forte dans votre organisation et ceci à faible coût.

La solution **IDCONFIRM 1000** de Gemalto propose différentes méthodes d'authentification aux ressources informatiques :

- Via un code à usage unique récupéré via une application sur smartphone
- Via un code à usage unique envoyé par SMS
- Via un code à usage unique récupéré sur un token au format porte-clés
- Via une carte à puce

IDConfirm fonctionne avec de multiples systèmes d'exploitation et configurations de serveur, il s'intègre de manière transparente dans les architectures existantes, y compris RADIUS (Remote Authentication Dial-In Server), AAA (Authentication, Authorization and Accounting) et des serveurs d'applications Web.

Pour assurer le niveau le plus avancé de protection de l'identité de l'utilisateur, le module de sécurité du logiciel IDConfirm ou un module de sécurité matériel externe (HSM) est lié à un serveur d'authentification pour stocker et utiliser des clés cryptographiques.

En utilisant des framework et des protocoles tels que HTTP / HTTPS et RADIUS standard, les modules d'authentification interagissent avec les serveurs de données existants afin de maintenir et de mettre à jour les informations d'authentification des utilisateurs. Plusieurs options de base de données et de répertoires sont supportées.

Systèmes d'exploitation

- Windows 2012 et 2012 R2
- Windows Server 2008 R2
- Red Hat Linux

Méthodes d'authentification

IDConfirm utilise les méthodes suivantes pour l'authentification principale:

- OATH (Event based, Time based)
- SMS OTP
- EMV CAP

Serveurs Web

- Apache Tomcat
- IBM WebSphere

L'architecture choisie permet la configuration "haute disponibilité" et "Fail-Over" en s'appuyant sur les systèmes d'exploitation, les bases de données et des mécanismes de suivi.

Bases de données

IdConfirm stocke les données relatives aux OTP et les données d'utilisateurs si besoin dans :

- MS SQL
- Oracle
- MySQL
- Firebird
- Toute autre base de données pourrait être supportée avec un développement spécifique

Répertoire d'utilisateurs

IDConfirm peut être connecté aux LDAP suivants quand les comptes utilisateurs sont gérés en externe:

- Microsoft Active Directory
- Novell eDirectory
- Open LDAP
- Tout autre LDAP pourrait être supporté avec un développement spécifique

Interface de services d'authentification

Les services d'authentification sont intégrés en utilisant les interfaces suivantes:

- Web Service REST API
- Requêtes RADIUS via IDConfirm:
- Microsoft NPS
- FreeRADIUS
- AD FS MFA Adapter