

DigiCert® Enterprise PKI Platform est désormais compatible avec Windows Hello Entreprise

L'authentification sans mot de passe, des arguments séduisants

L'authentification sans mot de passe renforce la sécurité au niveau des points d'accès tout en simplifiant le processus de connexion pour les utilisateurs. Pas étonnant, donc, que cette méthode d'authentification connaisse un tel engouement. Attaques par rejeu, tentatives de phishing, divulgations suite au piratage d'un serveur... Aucun mot de passe, aussi fort soit-il, n'est inviolable. Sans parler des combinaisons difficiles à mémoriser pour les utilisateurs. À l'heure où le modèle Zero Trust s'impose dans les entreprises, chaque demande d'accès est désormais soumise à vérification. En ce sens, la sécurité des accès devient un enjeu majeur pour protéger contre les attaques sans entraver les performances et la productivité des salariés. Avec l'authentification sans mot de passe, fini le casse-tête de la création et de la mémorisation de mots de passe : l'identité des utilisateurs est vérifiée par des méthodes de connexion plus sécurisées.

Windows Hello Entreprise : un modèle de confiance basé sur les certificats

Windows Hello Entreprise (WHfB) est une solution Microsoft d'authentification sans mot de passe qui consiste à vérifier la connexion des utilisateurs via une authentification multifacteur sur PC et appareils mobiles, notamment par biométrie ou code PIN.

Le modèle de confiance basé sur les certificats de WHfB fait appel à des certificats numériques reposant sur une infrastructure à clé publique (PKI, Public Key Infrastructure). L'authentification auprès du service Active Directory (AD) s'opère ainsi par le biais de certificats émis par une Autorité de certification (AC).

Le modèle de confiance par clé authentifie les utilisateurs auprès d'un AD à l'aide d'une clé et nécessite des certificats auto-signés.

Parmi les deux principaux modèles de confiance pris en charge par WHfB, à savoir le modèle par clé et le modèle par certificat, certaines entreprises privilégieront le second, notamment dans les scénarios suivants :

- Cas d'usage : dans le cadre du modèle de confiance par certificat, les certificats WHfB offrent les mêmes possibilités d'authentification qu'une carte à puce pour les ouvertures de session Windows.
- Technologie de gestion des identités et des accès (IAM) : les entreprises qui émettent et gèrent les certificats de leurs utilisateurs finaux à l'aide de leur propre infrastructure PKI peuvent utiliser leur infrastructure avec Windows Hello Entreprise.

“

89 %

des attaques réussies contre les applications web impliquent une compromission des identifiants de connexion (vol de mot de passe ou attaque par force brute) ”

-- Verizon 2021 Data Breach Investigation Report (DBIR)

DigiCert® Enterprise PKI Platform et Windows Hello Entreprise

Parce qu'elle est compatible avec le modèle de confiance basé sur les certificats proposé par WHfB, DigiCert Enterprise PKI Platform permet aux clients de mettre en œuvre les cas d'usage propres à l'authentification sans mot de passe, profitant ainsi de tous les avantages offerts par cette solution :

- **Simplification** de l'administration des certificats WHfB incluant des modèles de certificat préconfigurés et les méthodes d'enrôlement associées.
- **Accélération** de l'onboarding grâce à l'automatisation des flux et le provisionnement zero-touch (ZTP) de certificats d'authentification client requis par WHfB pour des appareils joints à un domaine Windows.
- **Centralisation** de la gestion des certificats numériques WHfB et des autres cas d'usage de l'entreprise sur une seule et même plateforme.

La prise en charge de WHfB vient compléter l'éventail de fonctionnalités proposées par DigiCert Enterprise PKI Platform pour aider les organisations à simplifier le provisionnement et l'administration des certificats numériques. Ces dernières peuvent ainsi automatiser leurs workflows, utiliser des modèles préconfigurés, choisir entre différentes méthodes d'enrôlement et tirer parti de l'intégration de solutions tierces.

Les avantages pour les administrateurs de Windows Hello Entreprise sont multiples :

Fonctionnalité de DigiCert Enterprise PKI Platform	Avantages
Modèles de certificats prédéfinis pour WHfB	Accélère l'onboarding des utilisateurs et des appareils via le serveur d'enrôlement automatique DigiCert (sans client) grâce à des modèles de certificat prédéfinis pour le contrôleur de domaine, l'agent d'enrôlement et l'authentification utilisateur de WHfB
Gestion zero-touch du cycle de vie des certificats	Augmente la productivité et la protection des utilisateurs grâce à une gestion automatisée des renouvellements, des réémissions, des expirations et du reprovisionnement des certificats
Protection optimale des clés et application des politiques	Offre différentes options pour la génération et la protection de clés via le Trusted Platform Module (TPM) et permet l'application de politiques imposant l'utilisation du TPM
Intégration transparente aux systèmes et applications tiers de WHfB	Prend en charge les API REST, les protocoles SCEP et EST ainsi que le standard SAML pour les services fédérés et distribués
Administration et gestion centralisées des certificats numériques WHfB et autres	Offre une visibilité et un contrôle inégalés de l'écosystème de certificats à l'échelle de l'entreprise en regroupant sur une seule et même plateforme la gestion complète du cycle de vie des certificats, le suivi, les journaux d'audit et le reporting
Déploiement rapide de la plateforme	Accélère le déploiement et la création d'Autorités de certification en ligne, qu'elles soient logicielles ou basées sur des modules de sécurité matérielle (HSM)
Plateforme PKI hautement flexible et évolutive	Propose plusieurs options de déploiement de la plateforme PKI avec une évolutivité éprouvée : en cloud, sur site ou en modèle hybride
Prise en charge multilingue	Offre une prise en charge multilingue sur l'ensemble des interfaces web, des consoles d'administration et des pages web utilisées pour l'enrôlement des utilisateurs.

Configuration technique requise

Versions DigiCert® Enterprise PKI Platform :

- DigiCert PKI Platform 8 avec serveur d'enrôlement automatique sur un serveur Windows joint à un domaine* ou
- Enterprise PKI Manager avec serveur d'enrôlement automatique sur un serveur Windows joint à un domaine (disponible à partir du 1er trimestre 2022)

Systèmes d'exploitation (OS) Windows Server : 2019, 2016 ou 2012

Services d'annuaire :

Windows Active Directory (AD)*, Azure AD

Solution d'authentification unique (SSO) :

Services de fédération Microsoft Active Directory (ADFS)

Solution de synchronisation des données d'identité :

Azure AD Connect

OS de la machine cliente :

Windows 10

*Les composants doivent être exécutés sur la même version du système d'exploitation Windows Server

Pour plus d'informations, contactez-nous par le biais du formulaire sur la page <https://www.digicert.com/fr/digicert-enterprise-pki-manager/>.