DigiCert® PKI-Plattformen für Unternehmen: Unterstützung für Windows Hello for Business

Lieber passwortfrei?

Die passwortfreie Authentifizierung wird immer beliebter, um die Sicherheit am Zugriffspunkt zu verbessern und gleichzeitig die benutzerseitige Anmeldung zu vereinfachen. Selbst die stärksten Passwörter helfen nicht, wenn sie während der Eingabe mitgeschnitten werden. Auch bei Phishing-Angriffen oder serverseitigen Sicherheitsverletzungen bieten sie keinen Schutz. Ganz zu schweigen davon, dass sich Benutzer ihre Passwörter auch merken müssen ... Zudem steigen viele Unternehmen auf ein Zero-Trust-Modell um, bei dem jede Zugriffsanforderung einzeln verifiziert wird. Die Zugriffssicherheit wird also beim Schutz vor Angriffen immer größer geschrieben. Passwortfreie Authentifizierung bedeutet, dass Benutzer keine Passwörter mehr erstellen und speichern müssen. Stattdessen wird die Benutzeridentität durch zuverlässigere Methoden überprüft.

> **89 %**
>
> **der beobachteten Sicherheitsverletzungen bei Webanwendungen waren auf den Missbrauch von Anmeldedaten zurückzuführen (gestohlene Zugangsdaten oder Brute-Force-Angriffe).**
>
> Verizon Data Breach Investigation Report 2021

Windows Hello for Business: das zertifikatsbasierte Vertrauensmodell

Windows Hello for Business (WHfB) ist eine Lösung von Microsoft für die passwortfreie Authentifizierung bei Anmeldevorgängen auf PCs und Mobilgeräten, die eine starke (Multifaktor-)Authentifizierung in Kombination mit biometrischen oder PIN-basierten Anmeldeverfahren nutzt.

Das zertifikatsbasierte Vertrauensmodell für WHfB nutzt digitale, von einer Zertifizierungsstelle (Certificate Authority, CA) ausgestellte Zertifikate innerhalb einer PKI (Public Key Infrastructure) für die Authentifizierung bei Active Directory (AD).

Beim schlüsselbasierten Vertrauensmodell erfolgt die Authentifizierung bei Active Directory hingegen über einen Schlüssel und selbstsignierte Zertifikate.

WHfB unterstützt also beide Modelle, die schlüsselbasierte und die zertifikatsbasierte Authentifizierung. In der Regel bevorzugen Unternehmen das zertifikatsbasierte Modell, wenn …

- bestimmte Anwendungsfälle erfüllt werden müssen: Beim zertifikatsbasierten Vertrauensmodell kann ein WHfB-Zertifikat für die Anmeldung bei Windows genau wie eine Smartcard verwendet werden.
- Technologie für die Identitätsprüfung und den Zugriff vorhanden ist: Unternehmen, die bereits eine PKI zum Ausgeben und Verwalten von Endbenutzerzertifikaten verwenden, können ihre PKI zusammen mit Windows Hello for Business nutzen.

DigiCert® PKI-Plattformen für Unternehmen und Windows Hello for Business

Die DigiCert PKI-Plattformen für Unternehmen unterstützen das zertifikatsbasierte Vertrauensmodell für WHfB und die damit verbundenen Anwendungsbereiche. So erhalten Kunden die Vorteile passwortfreier Authentifizierungsinitiativen, darunter:

- **Vereinfachte Zertifikatsverwaltung** für WHfB mit vorkonfigurierten Zertifikatsvorlagen und Registrierungsmethoden
- **Beschleunigte Zertifikatsausstellung** durch automatisierte Workflows und Zero-Touch-Bereitstellung der clientseitig authentifizierten Zertifikate, die WHfB zur Zugriffskontrolle auf Workstations einer Domain und Domaincontrollern benötigt
- **Anwenderfreundliche Verwaltung** von WHfB-Zertifikaten über eine bereits im Unternehmen verwendete Plattform

Die Unterstützung von WHfB ist nur eine der zahlreichen Funktionen der PKI-Plattformen von DigiCert, die die Bereitstellung und Verwaltung von digitalen Zertifikaten in Unternehmensumgebungen vereinfachen – basierend auf automatisierten Workflows, vorkonfigurierten Vorlagen, Unterstützung mehrerer Registrierungsmethoden und Integrationsfreundlichkeit für Drittanbieterlösungen.

Administratoren von Windows Hello for Business profitieren auf folgende Weise:

Eigenschaft der PKI-Plattform	Vorteile
Vordefinierte Zertifikatsvorlagen für WHfB	Beschleunigte Einbindung von Benutzern und Geräten über den clientlosen DigiCert-Server für die automatische Registrierung mit vordefinierten Zertifikatsvorlagen für die Authentifizierung von Registrierungsagenten, Benutzern und der von WHfB benötigten Domaincontroller
Zero-Touch-Management im gesamten Zertifikatslebenszyklus	Höhere Benutzerproduktivität und stärkere Sicherheit dank automatisierter Funktionen für die Erneuerung und Neuausstellung von Zertifikaten sowie die Verwaltung von Ablauffristen
Starke Schlüssel und Richtliniendurchsetzung	Optionen für die Erzeugung und den Schutz von Schlüsseln durch TPM (Trusted Platform Module) sowie Richtliniendurchsetzung für die Verwendung von TPM
Nahtlose Integration mit von WHfB unterstützten Drittanbietersystemen und -anwendungen	Integrationsfreundlichkeit dank Unterstützung von REST-APIs, SCEP und EST sowie SAML für verbundene und verteilte Services
Zentralisierte Verwaltung für WHfB-basierte und andere digitale Zertifikate	Transparenz und Kontrolle über die unternehmensweite Zertifikatslandschaft mit umfassenden Funktionen für die Verwaltung des Zertifikatslebenszyklus, Nachverfolgung, Berichterstellung und Audit-Logs über eine zentrale Plattform
Schnelle, plattformbasierte Bereitstellung	Beschleunigte Bereitstellung und Erstellung einer Online-Zertifizierungsstelle für software- und HSM-basierte Zertifizierungsstellen
Extrem flexible und skalierbare PKI-Plattform	Mehrere Bereitstellungsoptionen und bewährte Skalierbarkeit für die PKI-Plattform, einschließlich Modellen für Cloud-, Hybrid- und On-Premises-Umgebungen
Unterstützung mehrerer Sprachen	Unterstützung mehrerer Sprachen für alle Webschnittstellen, Verwaltungskonsolen und Webseiten für die Benutzerregistrierung

Technische Anforderungen

DigiCert® PKI-Plattformen für Unternehmen:	• PKI Platform 8 mit Server für die automatische Registrierung auf Windows Server (mit Domain-Anbindung)* oder • Enterprise PKI Manager mit Server für die automatische Registrierung auf Windows Server (mit Domain-Anbindung), verfügbar ab 1. Quartal 2022
Betriebssystemversionen für Windows Server:	2019, 2016 oder 2012
Verzeichnisdienst:	Windows Active Directory (AD)*, Azure AD
SSO-Lösung (Single Sign-On):	Microsoft Active Directory Federation Services (ADFS)
Lösung für die Synchronisierung von Identitätsdaten:	Azure AD Connect
Betriebssystem des Client:	Windows 10

* Die Komponenten müssen unter derselben unterstützten Version von Windows Server ausgeführt werden.

Weitere Informationen erhalten Sie über das Formular unter **https://www.digicert.com/de/pki/enterprise-pki-manager**.