DigiCert® Enterprise PKI-platformen en Windows Hello voor Bedrijven

Weg met wachtwoorden!

Wachtwoordvrije authenticatie wordt steeds populairder als methode om de beveiliging op het punt van toegang te verbeteren en het de gebruiker gemakkelijker te maken. Ook sterke wachtwoorden kunnen worden onderschept, gestolen door middel van een phishingaanval of op straat komen te liggen na een datalek. Daarnaast zijn ze vaak lastig om te onthouden. Bedrijven baseren hun beveiliging steeds vaker op het concept 'zero trust', wat inhoudt dat elk toegangsverzoek tot het netwerk moet worden gecontroleerd. Om een bedrijf te beschermen tegen aanvallen en ervoor te zorgen dat medewerkers hun werk kunnen doen, heeft de beveiliging van toegang dus een hoge prioriteit. Met wachtwoordvrije authenticatie hoeven gebruikers geen wachtwoorden meer aan te maken en te onthouden, en kunnen ze veiligere methoden gebruiken voor het verifiëren van identiteit.

> **89%**
>
> **van de inbreuken op webapplicaties is het gevolg van het misbruik van inloggegevens (gestolen gegevens of brute force).**
>
> --Verizon 2021 Data Breach Investigation Report

Windows Hello voor Bedrijven: het certificaatvertrouwensmodel

Windows Hello voor Bedrijven (WHvB) is een Microsoft-oplossing voor het wachtwoordvrij aanmelden op pc's en mobiele apparaten, die gebruikmaakt van meervoudige authenticatie, biometrie en pincodes.

Het certificaatvertrouwensmodel voor WHvB werkt op basis van digitale certificaten in een Public Key Infrastructure (PKI), die worden gebruikt voor de authenticatie bij Active Directory (AD) met certificaten die zijn uitgegeven door een certificeringsinstantie (CA).

In het sleutelvertrouwensmodel vindt de authenticatie bij AD plaats met behulp van een sleutel en de daarvoor vereiste zelfondertekende certificaten.

Van de twee vertrouwensmodellen die worden gebruikt door WHvB, is het certificaatvertrouwensmodel het meest geschikt voor bedrijven waarvoor de volgende zaken belangrijk zijn.

- Gebruiksscenario's: in het certificaatvertrouwensmodel kan een WHvB-certificaat net als een smartcardcertificaat worden gebruikt voor het aanmelden bij Windows.
- Identiteits- en toegangstechnologie: bedrijven die al gebruikmaken van PKI voor het uitgeven en beheren van eindgebruikerscertificaten kunnen hun PKI ook gebruiken in combinatie met Windows Hello voor Bedrijven.

DigiCert® Enterprise PKI-platformen en Windows Hello voor Bedrijven

De grootzakelijke PKI-platformen van DigiCert bieden ondersteuning voor het certificaatvertrouwensmodel van WHvB. Daarmee faciliteren ze de gewenste gebruiksscenario's binnen bedrijven, zodat die eenvoudig kunnen overstappen op wachtwoordvrije authenticatie. Dat biedt de volgende mogelijkheden:

- **Eenvoudige WHvB-certificaatadministratie** dankzij vooraf geconfigureerde sjablonen en bijbehorende registratiemethoden.
- **Snelle onboarding** met geautomatiseerde workflows en zero-touch provisioning van geauthenticeerde clientcertificaten, die WHvB vereist voor workstations in een Windows-domein.
- **Gemakkelijk beheer** van digitale WHvB-certificaten met het platform dat ook wordt gebruikt voor de andere certificaten binnen het bedrijf.

De ondersteuning voor Windows Hello voor Bedrijven is een van de vele mogelijkheden van de DigiCert PKI-platformen. Dankzij die platformen beschikken bedrijven over eenvoudige uitgifte en beheer van digitale certificaten met behulp van geautomatiseerde workflows, vooraf geconfigureerde sjablonen, meerdere registratiemethoden en integratie met oplossingen van derden.

Voor beheerders van Windows Hello voor Bedrijven biedt dit de volgende voordelen:

Functie van PKI Platform	Voordeel
Vooraf gedefinieerde certificaatsjablonen voor WHvB	Snelle onboarding van gebruikers en apparaten via de registratieserver van DigiCert met vooraf gedefinieerde certificaatsjablonen voor WHvB-domeincontrollers, registratieagents en gebruikersauthenticatie
Zero-touch levenscyclusbeheer van certificaten	Verbetert de productiviteit en beveiliging met mogelijkheden voor het automatisch verlengen, opnieuw uitgeven en intrekken van certificaten
Krachtige sleutelbeveiliging en beleidshandhaving	Biedt opties voor het genereren en beveiligen van sleutels met een Trusted Platform Module (TPM) en het handhaven van beleid met een TPM
Complete integratie met WHvB-systemen en -applicaties van derden	Eenvoudige integratie dankzij ondersteuning voor REST API, SCEP, EST en SAML voor gemeenschappelijke en gedistribueerde services
Centrale administratie en beheer voor WHvB-certificaten en andere digitale certificaten	Geeft een compleet beeld van en goede controle over alle certificaten die binnen het bedrijf in gebruik zijn, dankzij volledig levenscyclusbeheer, bewaking, auditlogboeken en rapportages in één centraal platform
Snelle platformimplementatie	Faciliteert snelle implementatie en het opzetten van online certificeringsinstanties, zowel softwarematig als op basis van een HSM (Hardware Security Model)
Zeer flexibel en schaalbaar PKI-platform	Ondersteuning voor meerdere, uitstekend schaalbare implementatieopties: in de cloud, on-premises en hybride vormen
Meertalige ondersteuning	Ondersteuning voor meerdere talen in alle webinterfaces, beheerconsoles en registratiepagina's voor gebruikers.

Technische vereisten

DigiCert® Enterprise PKI-platformen:	• PKI Platform 8 met Auto-Enrollment Server op een Windows Server binnen een domein* of • Enterprise PKI Manager met Auto-Enrollment Server op een Windows Server binnen een domein (verkrijgbaar vanaf eerste kwartaal 2022)
Windows Server-besturingssystemen:	2019, 2016 of 2012
Directory Service:	Windows Active Directory (AD)*, Azure AD
Oplossing voor single sign-on:	Microsoft Active Directory Federation Services (ADFS)
Oplossing voor synchronisatie van identiteitsgegevens:	Azure AD Connect
Besturingssysteem clientmachines:	Windows 10

*Alle onderdelen moeten worden uitgevoerd op hetzelfde Windows Server-besturingssysteem

Wilt u meer informatie? Ga naar **https://www.digicert.com/nl/** en vul het formulier in.