HID® Credential Management Service Provides Credentialing & Authentication for Companies That Need to Continue Supporting PKI Access to Azure Services

HID Credential Management Service is the identity and access management solution for organizations reliant on on-premises active directory (AD) and public key infrastructure (PKI) technologies that need to provide user credentialing and authentication to applications and services running on the Microsoft Azure cloud environment. Underpinning HID’s Certificate-Based Authentication to Azure AD service, HID CMS is the ideal alternative for organizations that continue to rely on centrally stored passwords, and are not yet prepared to transition to the Windows Hello service that’s based on FIDO-certified security.

Toward a Passwordless Future

Microsoft has been at the forefront of tech industry efforts to move away from password-based credentialing, access management and authentication. As part of these efforts, Microsoft announced in the Spring of 2019 that it had adopted FIDO-certified security into its Windows Hello login platform. As such, Windows 10 users can move beyond centrally-stored passwords and leverage Windows Hello biometrics or PINs to access their devices, apps, online services and networks.

A lesser-publicized contingency of the FIDO announcement was that Microsoft would no longer support conventional PKI for accessing applications and resources within its popular Azure cloud environment. This presented a dilemma for organizations reliant on PKI and conventional on-premises active directory-based technologies for user credentialing and authentication. With most large organizations today embracing multi-cloud strategies, and often running key applications and resources in the Azure environment, many faced the prospect of having users cut off from business-critical systems and data.

An Enduring Legacy for PKI

HID Global is offering a solution for companies facing the Azure PKI deprecation problem: HID® Certificate-Based Authentication to Azure AD. Built up from the HID® Credential Management Service, this new Azure-specific solution enables organizations to issue authentication credentials that go beyond perimeter security. Clients can choose from smart cards, smart USB keys, Windows® TPMs and mobile phones for secure access to applications hosted on the Azure platform, as well as individual workstations and servers within the firewall, and VPNs.
How It Works – PKI Certificate Based Authentication to Azure AD

Let’s walk through a use case scenario where an organization would need to provide user access to an application on Azure, which supports SSO from Azure AD.

**Solution Components**

Authentication of PKI credentials from within Azure

**The solution would be based on two core components:**
- HID Credential Management Service for the issuance and management of PKI credentials to smart card or mobile app.
- A DigitalPersona server for the authentication of PKI credentials from within Azure.

**High-Level Solution Overview**

With the user and the user’s devices at the center of the authentication loop, the process would draw on HID Cloud Infrastructure resources:
- HID IdenTrust to provide digital certificates.
- HID Credential Management Service to issue credentials.

**Card / Mobile Issuance**

For the issuance of the credentials:
- User logs into the HID Credential Management Service Portal.
- User inserts Crescendo Card into reader or downloads Crescendo Mobile App and connects the Mobile App via Bluetooth or NFC to the PC.
- User starts Crescendo Card or Crescendo mobile issuance in HID Credential Management Service Portal.
- 4. HID Credential Management Service requests a Certificate from IdenTrust CA.
- 5. The certificate is loaded to the Smart Card or Mobile App on the smartphone.
For the authentication:

- User opens browser to navigate to its online application login portal leveraging Azure AD as the IdP.
- The user is directed to Azure AD.
- Azure AD does not natively support PKI authentication and therefore is configured to redirect the user to the DigitalPersona IDP Portal with WS-Federation.
- The user arrives at the DigitalPersona IDP Portal and is prompted to provide a PKI credential.
- The user inserts their smartcard into their PC or loads their virtual smart card on their mobile device and connects the device to the PC via Bluetooth or NFC.
- DigitalPersona Authenticates the Certificate.
- DigitalPersona provides a success message to Azure AD.
- Azure AD redirects the authenticated user to its online application.

“Real” Solution Overview

A map of the complete authentication loop architecture.

HID Credential Management Service Benefits

HID® Credential Management Service provides organizations with comprehensive, highly configurable solutions to meet their unique needs. With HID Global, organizations can establish trust in the identity of users to securely manage access to all their networks, PCs, in-house, public and private cloud applications - including applications running on Azure - building facilities, and other resources. With the HID Credential Management Solution, organizations can switch from Active Directory on premise to Azure AD while keeping their PKI deployment enabled for authentication. This means your organization can make a smooth transition to the cloud without enduring a wrenching, expensive “rip & replace” exercise. Moreover, HID Global stands ready to continue supporting your transition to passwordless authentication via Microsoft Hello with our range of solutions that integrate FIDO credentials into different form factors, including smart cards, mobile apps, USB dongles and more.
HID Credential Management Service enables the usage of digital identities for secure multi-factor authentication, digital signature and encryption. It provides a complete flexible solution to meet the organization’s security policies and IT’s architecture requirements. HID CMS can deploy a variety of authenticators, including smart cards, smart USB keys and mobile devices. Each of those authenticators can protect multiple credentials, including public key infrastructure (PKI) certificates, FIDO and one-time passwords (OTPs). They can also be used for Physical Access Management. HID Credential Management Service provides the full range of identity and access management features and capabilities needed to provide user credentialing and authentication to applications and services running on the Microsoft Azure cloud environment, including:

- A single platform capable of issuing and managing HID Global authenticators that increases security and reduces fraud.
- Proven technology used by numerous security-minded organizations to issue hundreds of millions of credentials.
- Choice of authenticator form factor: smart cards, smart USB keys and mobile devices.
- Customizable workflows and policies that readily adapt to a variety of environments and deployment scenarios.
- Unique, patented post-issuance update capabilities allow organizations to extend the lifetime of authenticators, offering cost-savings and productivity enhancements.
- Web-based help desk administration.
- Tamper-evident audit features that log all event activities for reporting.
- Compliance with stringent U.S. Federal Government Personal Identity Verification (PIV) standards including derived PIV credentials.
- Easy integration with a wide variety of directories, front or backend identity management and provisioning systems, certificate authorities, and physical access control systems.
- Extensibility to support batch and service bureau issuance models.

For more information, visit: http://www.hidglobal.com