High Assurance Authentication that Empowers User Experiences

Discover HID Global's Strategic Approach to Security that Combines Public Key Tokens with Comprehensive Credential Management and Azure Active Directory Certificate-Based Authentication (Azure AD CBA) for Greater Protection and Enhanced Employee Productivity

Microsoft

Contents

Why Now Is the Right Time to Reconsider Your Identity Security

Digital Drives Change

A new era has dawned. Nearly every business communicates and interacts online. Remote and hybrid work has surged as a result of the pandemic. And many organizations are actively moving more of their processes to the cloud to sustain business continuity and keep employees connected and productive no matter their location, including:

- 99% of organizations were using one or more SaaS (software as a service) solutions at the end of 2021.[1]
- 94% of today's enterprises use cloud services.[2]
- 92% of organizations had a multi-cloud strategy in 2021.[3]

Most of us have embraced these digital trends out of necessity. But we may not have initially noted some of the challenges that come with digital transformation. Namely, it is difficult for organizations with a variety of apps, systems, and networks to balance user experience with the need for greater security — especially in light of evolving industry regulations and mandates.

The recent White House Executive Order on Improving the Nation's Cybersecurity Infrastructure is one example of how important Zero Trust is becoming to nations around the globe with governments calling for higher levels of security to protect critical infrastructure from cyberthreats. Both organizations and governments need a Zero Trust security model to thrive in today's world. That means taking a no-trust approach to cybersecurity and implementing phishing-resistant authentication processes like Multi-Factor Authentication to ensure the protection of every person, device, app, and data wherever they are located.

Think Beyond Passwords

Managing the influx of new and old user identities and access permissions across your organization is challenging. And it has not been made easier by cybercriminals who are becoming more skilled at stealing identities, including:

- 85% of breaches in 2021 involved the human element.[4]
- Compromised passwords account for more than 60% of data breaches.[4]

There is no denying that modern businesses need stronger authentication protocols to govern access to critical resources like company devices, networks, legacy apps, cloud services, and even physical entities like buildings and rooms. But if you are unable to see and manage access policies for every employee and customer, security errors such as weak passwords and system access oversights can give an attacker everything they need to access your data.

Build a Comprehensive Security Strategy for 2022

Every company needs to enable secure access, whether that is to cloud applications like Microsoft 365, legacy applications, encrypted emails, printers, physical offices, or others. Standards like Fast Identity Online (FIDO), public key infrastructure (PKI), and the Initiative for Open Authentication (OATH) are helping IT teams strengthen their approach to identity authentication. Yet adoption of these protocols is not easy and tends to happen at different paces, with some subsuming others over time. Not every company hires security experts proficient enough in systems architecture and security standards to navigate those complexities.

To give companies a comprehensive approach to security, HID Global has collaborated with Microsoft to enable certificate-based authentication (CBA) in Azure Active Directory (Azure AD) environments. This is achieved by integrating Azure AD CBA with Crescendo® smart cards and security keys as well as centralized credential management with the cloud-based WorkforceID™ Digital Credential Manager. The combination of these HID® product lines with Azure AD CBA supports multiple security standards and communication protocols to help IT admins take advantage of three key benefits that are crucial to striking the right balance between exceptional employee experiences and heightened protection.

Learn More

Phishing-Resistant Authentication

Enable seamless, protected access to corporate resources.

Learn More

Seamlessly Manage Your Hybrid Workforce

Drive remote productivity while managing credential lifecycles.

Learn More

Secure Access to non-FIDO Enabled Resources

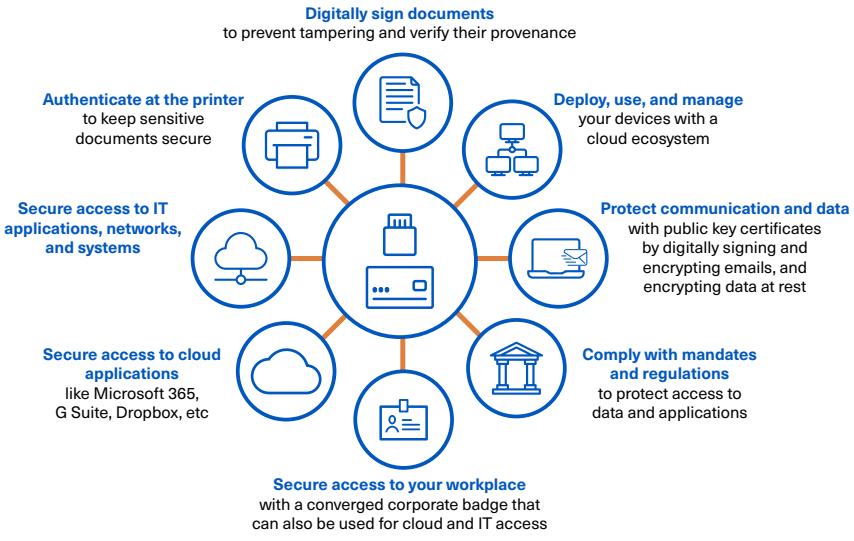
Enable stronger authentication for legacy applications.

Phishing-Resistant Authentication

How do you provide attack-proofed access to countless corporate resources?

The first step toward stronger authentication and a Zero Trust security model is finding solutions that comply with FIDO2, an open security protocol that is entirely focused on eliminating the major cause of breaches and security incidents: passwords. Passwords continue to be one of the top vulnerabilities affecting IT systems, with credential theft accounting for 37% of all breaches.[4] Passwords are not only a liability; they are also a hassle to replace and manage. That is why more organizations are exploring public and private key cryptography and multi-factor authentication to move away from password-related risks.

With FIDO2, PKI/PIV, OATH, and physical access capabilities, Crescendo smart cards and security keys help organizations meet regulatory compliance with an easy-to-adopt and fast-to-deploy multi-factor authentication solution. Additionally, users can self-enroll credentials via WorkforceID Digital Credential Manager, which securely manages provisioning, deprovisioning, and updating of user certificates, alleviating some of the onus of security administrators who can then enable certificate-based authentication for the appropriate business applications. Designed to integrate seamlessly with Azure AD CBA, organizations can take identity security a step further leveraging the granular Azure AD Conditional Access policy to determine when a certificate presented by an Azure AD user meets MFA requirements. The combination means organizations can accelerate a transition to passwordless authentication by deploying phishing-resistant credentials that eliminate risky, knowledge-based ones.



More Secure Identities and Access with Crescendo and Azure AD

All it takes is a few configurations in Azure AD and the registration of user credentials via the Self-Service Portal or an API.

Validate Crescendo public key tokens with Azure AD to:

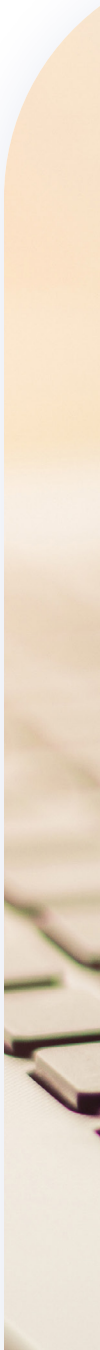
- Access Microsoft 365 and Power Apps.
- Authenticate to both cloud and on-premises resources.
- Digitally sign documents and emails.
- Encrypt data at rest and in transit.
- Securely access facilities and IT resources with the convenience of a single Crescendo smart card.

Seamlessly Manage Your Hybrid Workforce

How do you ensure access to sensitive data and corporate VPNs is not abused?

The next step in creating a more robust security stance in a dynamic workplace is embracing device and PKI-credential management as an added layer to your authentication process. In the context of remote and hybrid workforces, it can be difficult for companies to remotely issue and manage credentials. Enabling users to self-serve and enroll their own credentials from anywhere reduces the burden and dependency on IT administrators. However, it takes centralized management like WorkforceID Digital Credential Manager to ensure an organization retains full visibility into every hardware- and software-based credential that has access to digital and physical resources.

While Crescendo authenticators can be deployed on their own, organizations benefit more when they can manage the entire credential lifecycle centrally to ensure access to sensitive data and corporate networks is never abused or compromised by anyone. This is where centralized credential management, whether from the cloud (WorkforceID Digital Credential Manager) or on-premises (ActivID® Credential Management System) comes in handy. Organizations can use this solution to synchronize the issuance, replacement, and revocation of all their Azure AD user identities as well as their associated PKI certificates and hardware devices — all while remaining compliant with enterprise security policies.



Benefits of Using Public Key Infrastructure

With users working anywhere, embracing standards-based and widely adopted public key authenticators (PKIs) are more critical than ever to secure access to resources both within and outside the corporate firewall. Every employee, application, and device must have an identity and associated credentials that can be verified, trusted, and efficiently managed. Cloud-based services such as WorkforceID Digital Credential Manager help organizations boost security, performance, and availability on a global scale, while supporting rigorous NIST, ISO 27001, and GDPR compliance.

Secure Access to non-FIDO Enabled Resources

How do you securely provision access to legacy applications that are not FIDO enabled?

While FIDO2 support is growing and X.509, a standard format for public key certificates, has long provided a means for strong authentication, the reality is that most enterprises continue to maintain legacy applications. Your organization might run on critical infrastructure that cannot easily be migrated to the cloud. Still, you need a way to secure those applications since continued reliance on password-only authentication increases their threat profile. To bring your legacy applications under the protection of a comprehensive security strategy, you will need a solution that replaces passwords, but the last thing a company wants is yet another product to manage. What if you could get a single solution to address every authentication use case, from logical to physical access requirements?

In scenarios where companies use legacy enterprise applications, including in-house developed applications and VPN solutions with static passwords, Crescendo security keys can replace or augment static passwords with one-time passwords to increase security and pave the road to Zero Trust. Crescendo security keys can store an OATH-based credential, validated by an authentication service or server, allowing for increased security without a significant negative impact on the overall user experience or a need to replace existing infrastructure. If the application is connected to Azure AD, Crescendo security keys can also provide certificate-based authentication through Azure AD CBA.

Transform Identity and Access Management

Empower your employees to work the way they want while still enforcing strong security standards that keep your business safe.

- Secure access to digital resources and corporate facilities like buildings, floors, or rooms with the convenience of a single authentication device, Crescendo smart cards.
- Improve security in your dynamic workplace with proven device and PKI-credential management via a single platform.
- Resist phishing with Crescendo security keys and Azure AD CBA that work together to grant access to FIDO- or PKI-compliant apps without needing additional hardware.
- Connect your user directory by synchronizing Azure AD with your HID credential solutions.


Microsoft
Sign in with a security key
Your PC will open a security window. Follow the instructions there to sign in.
Windows Security
Making sure it's you
Please sign in to login.microsoft.com.
This request comes from Msedge, published by Microsoft Corporation.
Tap your security key on the reader or insert it into the USB port.
Cancel

Strong Authenticators Meet Centralized Identity Management

HID Global is one of the first vendors to provide credentials and credential management as a single packaged solution, empowering organizations to strike the right balance between seamless authentication experiences for faster login and instant access with centralized management of all user credentials. HID Global's powerful combination of credential authentication and management is designed to work with an organization's Microsoft technology stack, including Azure AD CBA — paving the road to Zero Trust.

Evaluate how Azure AD CBA and HID Global solutions can support your Zero Trust journey to drive strong authentication.

Learn about Microsoft Azure AD CBA

Learn more on the Azure Marketplace.

HID Crescendo Security Key

HID Crescendo Smart Card

WorkforceID Digital Credential Manager

[1] The State of SaaS in 2022: Growth Trends & Statistics, BMC
[2] 26 Cloud Computing Statistics, Facts & Trends for 2022, Cloudwards
[3] 2021 Flexera State of the Cloud Report
[4] 2021 Data Breach Investigations Report, Verizon

Part of ASSA ABLOY

Microsoft