EXECUTIVE BRIEF

HID Credential Management Service

Certificate-based authentication that's convenient for users and easy to deploy

Organizations that rely only on passwords for their user authentication are left vulnerable to password theft:

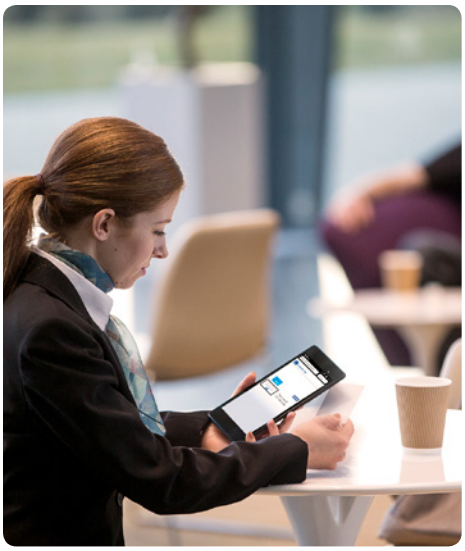
- Not only are lost or stolen passwords inconvenient, they are the leading cause of security breaches according to the Verizon Data Breach Investigation Report.
- As the instances of security breaches and their remediation costs increase each year, the potential threat of a catastrophic event impacting an organization's ability to do business is a risk that must be taken seriously.
- Reliance on passwords and complex password rules are inconvenient for users and costly to organizations. In addition to the increasing annual time and cost for password management by IT departments, the risks of fines for non-compliance and possible damages to brand reputation and customer loyalty are growing concerns.
- Governments and industry associations are reacting to this threat landscape with strict regulations and mandates that require stronger authentication approaches.
- With increasing fines and penalties mandated from regulations like the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act and the US Health Insurance Portability and Accountability Act (HIPPA), the costs to resolve a data breach can be overwhelming, on average $3.86 million in 2018 according to Ponemon Institute.

Some organizations already have deployed stronger methods of authentication, such as one-time passwords. But this authentication method is no longer adequate because it is easily breached and often focused only on an organization's network perimeter or Virtual Private Network (VPN) connections. It's no longer enough to focus on securing a perimeter around the organization. Today's organizations need a more holistic approach.

Savvy, cost efficient, IT organizations use certificate-based authentication to eliminate the burden of complex password rules while dramatically improving organizational security.

Historically, the complexity of deploying a complete certificate-based authentication solution, was cost efficient for only the largest organizations. HID Credential Management Service provides an easy and affordable way for organizations of all sizes to adopt certificate-based authentication with the following features:

- HID Credential Management Service is cloud-based, which means that organizations don't need to deploy or install a certification authority, a credential management system, or hardware security modules.
- HID Global manages the complexities of the public key infrastructure (PKI), so organizations can instantly provide certificate authenticators



to their users. These trusted certificates work seamlessly with most operating systems, browsers and applications.

- Since it is provided as a per user subscription model, HID Credential Management Service makes it possible for organizations to immediately adopt a solution without expensive up-front investments.

With HID Credential Management Service, you can choose the right authenticator for your employees' needs from several options including smart cards, smart USB keys and mobile apps that connect to users' PCs using Bluetooth.

The authenticator choice provides organizations options in term of security level, cost and convenience. Some authenticators can be used as a converged badge that allow users both physical access to buildings as well as logical access to the IT environment.

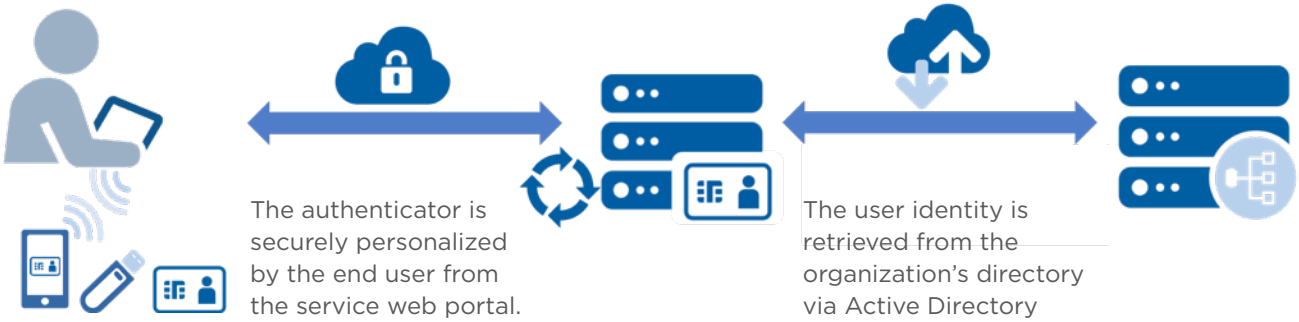
HID Credential Management Service Benefits:

- Eliminate complex password rules while improving your organization's security profile and employee efficiency.
- Protect your critical assets with stronger authentication, reducing risk from breaches and other security incidents.
- Deliver a single credential for systems, networks, and applications — reducing cost, complexity and providing a better user experience.
- Issue and manage credentials in the cloud removing the need to invest in new servers, new on-premise software licenses, or specialized IT expertise.
- Leverage certificate-based authentication to provide secure, easy to use, advanced capabilities like digital signature, email encryption and trusted identity management.
- Securely manage a large number of employees and contractors in dispersed locations, and update their credentials at any point in the life cycle.
- Provide higher security for VPNs, cloud applications and Microsoft Active Directory.
- Protect user authentication both inside and outside the organization's physical and logical perimeters.
- Experience peace of mind from a proven ecosystem that has issued and supported millions of credentials.

Authenticator options
Mobile smartcard (stored on a smartphone)
Crescendo FIPS smartcard *
Crescendo FIPS smartcard with physical access of choice *
Crescendo PIV smartcard *
Smart USB Key *

* FIPS 140-2 L2 certified

HID Credential Management Service – How It Works



The authenticator is securely personalized by the end user from the service web portal.

The user identity is retrieved from the organization's directory via Active Directory Federation Services.

The user securely authenticates from the device to Windows, cloud apps, VPN, and more. The user may also encrypt and digitally sign emails and documents sent from the device, ensuring privacy and mitigating risk.

2018-10-30-iam-hid-cms-cloud-solution-eb-en

PLT-04059