

Single Secure Credential to Access Facilities and IT Resources



HID PIV Solutions





Securing access to premises, applications and networks

Organizational Challenges

Organizations that want to secure access to their premises, applications and networks run into significant challenges:

- Passwords are insecure and costly to manage
- Physical and IT access are often silo'ed
- Users' digital identities are often not off-boarded when leaving the organization
- Organizations typically have multiple user populations with different needs

Government and regulated industries see security mandates and regulations tightening as the reporting of breaches increase. Unfortunately, the technology to address these issues can sometimes require products from up to 12 different vendors.

A Comprehensive Solution to Meet Your Identity and Access Needs

The HID PIV (Personal Identity Verification) solution addresses all those challenges by leveraging the same government-strength security solution that has already been deployed to more than seven million people across the world. Organizations benefit from the ecosystem created by this large footprint, with many applications, operating systems, and devices supporting natively the PIV credentials.

Customers can implement the HID PIV solution to be fully compliant with stringent mandates like PIV or PIV-Interoperable (PIV-I). If strict compliance to government mandates is not required, HID offers a lighter deployment model that still offers the increased security and interoperability of the PIV ecosystem.

Your organization benefits from a secure and reliable credential in the form of a smart card that can be used for visual identification, to protect access to facilities and access IT systems. Other form factor options are also available, including USB key, virtual smart card and derived credentials for mobile devices.

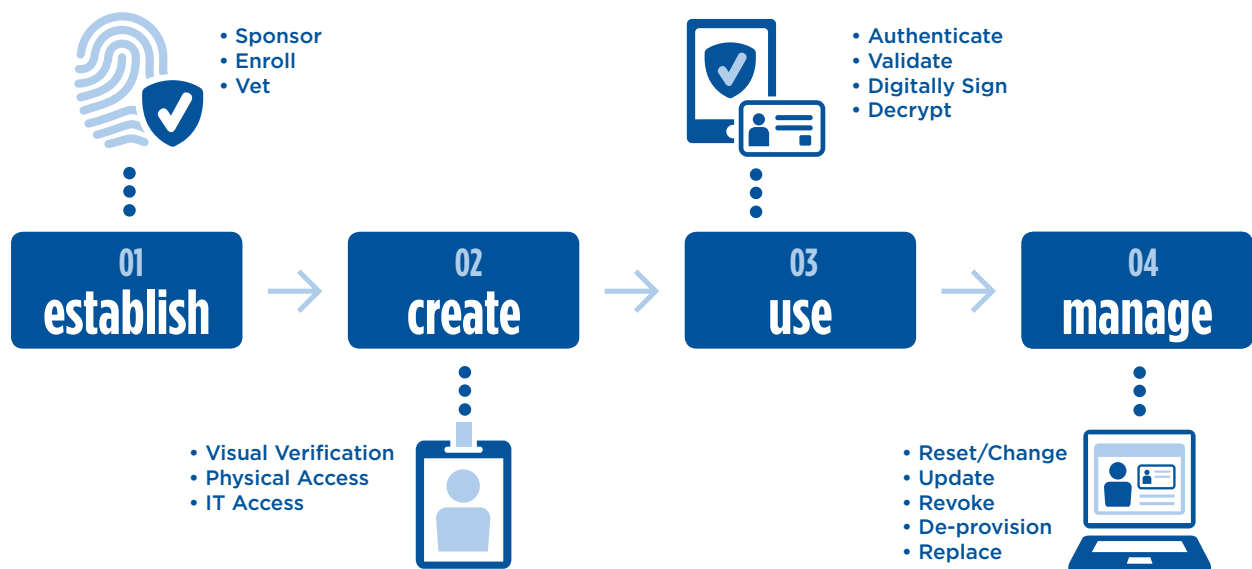
HID PIV Solutions Deliver:

- **Trusted Identity** - HID PIV provides your users with an identity that is trusted within your organization and can optionally be automatically trusted by other organizations you do business with.
- **Comprehensive Security** - HID PIV leverages the established strength of this existing standard and extends it to systems, networks, and applications resulting in a better security position for your organization.
- **Simplified User Experience** - By incorporating more capabilities into a single smart card or USB key, users have fewer credentials to remember or manage in order to get access to what they need to do their jobs, and are less likely to circumvent your controls.
- **Easier Deployment and Management** - The components of HID PIV are designed to work seamlessly together, so it is faster to get up and running, and easier to manage over time.
- **A Complete System** - HID PIV Enterprise encapsulates the entire PIV management process from establishing identity, to credential creation and issuance, synchronization of connected systems, and credential revocation.

HID PIV Solutions

- Trusted Identity
- Comprehensive Security
- Simplified User Experience
- Easier Deployment and Management
- A Complete Solution





Establish and Manage the Credential

What is PIV / PIV-I / HSPD-12 / FIPS 201 Compliance?

The US Federal government is mandated by Homeland Security Presidential Directive 12 (HSPD-12) that all federal employees and on-site contractors have a standard, secure, reliable form of identification. This form of identification is the Personal Identity Verification (PIV) card. PIV Interoperable (PIV-I) is a variation of that standard for non US Federal organizations that is still trusted by the US Federal government. FIPS 201 is the technical standard covering the processes to obtain such a card as well as the interoperability of such a card, including certification processes and listing the products approved by the US Federal Government. Derived Credentials also extend the PIV/PIV-I identity to mobile devices where the use of the card may be impractical.

Establishing the Identity – Root of Trust

Providing strong authentication starts by establishing the identity of the person that will receive the secure credential.

HID PIV Solutions can streamline this process by:

1. Integrating with authoritative sources such as HR or contractor management systems for automated sponsorship
2. Performing identity proofing (verifying and capturing approved state or national ID)
3. Enrolling the user fingerprint or iris data so that subsequent interaction with the system can be verified electronically without requiring the ID of the applicant
4. Connecting to external background check systems, including the United States Office of Personnel Management Federal Investigative Services
5. Adjudicating the application to determine if the applicant should receive the credential or not

HID PIV solutions provide a customizable HID PIV IDMS (Identity Management System) that is FIPS 201 compliant. Organizations that don't need to comply with PIV or PIV-I can configure the HID PIV solution to skip any of the above steps.

Credential Issuance & Lifecycle Management

Once an applicant has been approved to get a credential, HID PIV solution will securely issue that credential and manage its lifecycle. The credential itself can be in the form of a FIPS 140-2 certified smart card or USB key with embedded secure element. The smart card can be contact-only or dual interface (contact and contactless), which can be printed using an HID Fargo printer to include a facial image, personal information and/or organization logo. In addition to issuing and managing smart cards and USB keys, HID PIV can manage virtual and software credentials which are better suited for mobile computing devices such as tablets and smart phones. The credential typically contains digital certificates and the corresponding private keys, user data and an optional one-time password generator for legacy applications.

An additional component of HID PIV is ActivID® Credential Management System, which securely manages the lifecycle of the credential, including PIN unlock, certificate updates, credential lost/stolen/replacement, and termination. All updates can be done remotely in a highly secure fashion so that branch offices, remote or traveling employees and partners are serviced without requiring them to be physically present.



Credentials for Physical and IT Systems Access

Physical Access

The credential, when in a card form factor, can be used to access the organization premises.

Organizations typically have 2 options:

- Those that need full compliance with the PIV or PIV-I mandate: the card chip is accessible both via the contact and the contactless interface (also known as dual interface) and enables PKI authentication at the door
- Those that don't need full compliance with PIV or PIV-I but want to leverage their existing physical access system (PACS) and don't plan to deploy PKI authentication at the door: those organizations can use a combo card with the smart card contact chip for IT authentication and the PACS contactless chip for physical access

Organizations can also step up the security of specific doors by requiring 2 and 3 factor authentication including card presence, card presence + PIN entry or card presence + PIN entry + fingerprint validation.

HID PIV Enterprise can provide Physical Identity & Access Management (PIAM) to automatically provision and de-provision user access into your organization's PACS. HID PIV Enterprise supports

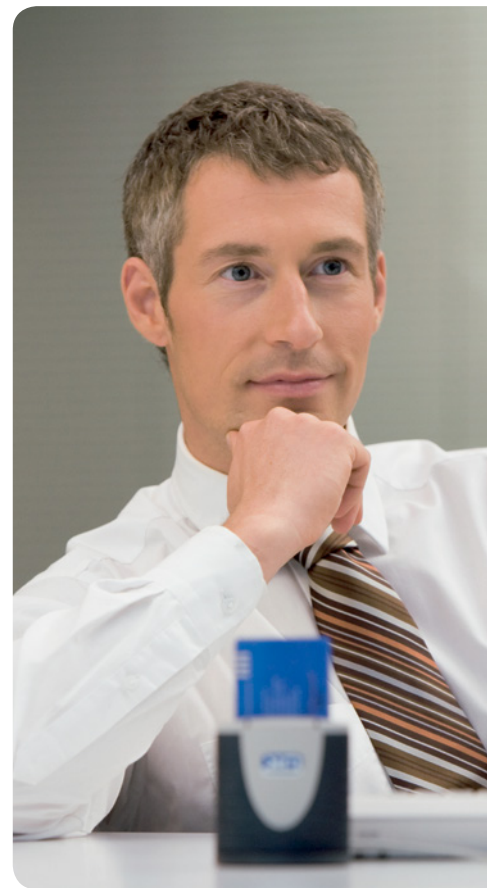
systems from many popular vendors so that large organizations that have many sites can manage the provisioning and de-provisioning of the users' identity and access privileges across the organization.

IT Systems Access

The same credential can be used to replace passwords with stronger authentication in many IT applications, including Microsoft Windows Active Directory, most VPN products, web sites, cloud applications, and more.

The user simply inserts his/her card into the smart card reader (or USB key) and types his/her PIN code to login for multi factor authentication. It will also lock itself after too many wrong attempts. The result is better security and better user convenience by eliminating complex, constantly changing passwords that are difficult to remember.

Mobile devices can also benefit from the seamless, improved security via virtual smart cards and derived credentials. Legacy applications that are not PKI enabled can often be supported using a One Time Password generated from the smart card and authenticated by an ActivID Appliance and then integrated into the application using protocols like RADIUS or SAML.





Deployment Options



HID PIV comes in two editions:

- **HID PIV Express™** is a customizable, easy to deploy, PIV compliant solution that does not require complex integration between point products
- **HID PIV Enterprise™** has all of the features of HID PIV Express but adds Physical Identity and Access Management (PIAM) capabilities. These advanced capabilities allow users to create a central PIV identity repository, automate access requirements based on policy rules that are enforced within your PACS systems. Additionally, HID PIV Enterprise includes enhanced process reporting to monitor and manage your credential workflows.

For maximum ease of procurement, deployment and maintenance, customers can take advantage of the full HID solution or leverage existing third party components to maximize existing investments.

HID PIV solutions help organizations improve their security posture, comply with mandates, improve the user experience, and is easier to procure, deploy and maintain.

For more information about HID PIV Express and Enterprise, please visit:

hidglobal.com/hidpiv

Advanced Use Cases

Users can also use their same credential to digital sign emails or documents, decrypt emails or files, protect their laptop with full disk encryption and boot protection, protect print jobs with secure printing and many other functions.

Organizations can optionally use IdenTrust® digital certificates so that their user's credentials are automatically trusted by virtually anybody that has a PC or mobile device.

North America: +1 512 776 9000 • Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800 • Latin America: +52 55 5081 1650

© 2017 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design, Genuine HID, iCLASS, PIV Enterprise and PIV Express are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

2017-11-15-iam-hidpiv-solutions-br-en PLT-03132

An ASSA ABLOY Group brand

ASSA ABLOY



hidglobal.com