DiGITAL TRUST
from Silicon to Services

intercede

MyID PIV enabling

Best practice from FIPS 201

Why choose MyID?

- IPS 201 approved market-leading product, successfully deployed in multiple federal agencies and used to issue millions of PIV cards
- Already in use for large scale PIV-interoperable and PIV-compatible (or CIV) deployments
- Flexible product, making PIV best practice work for your organization
- Issue PIV, PIV-I and CIV credentials from the same installation of MyID

What is PIV?

PIV stands for Personal Identity Verification, and is a term used to describe the process that US federal agencies go through in order to verify applicants' identities and issue trusted credentials to conform to the FIPS 201 standard. The FIPS 201 standard was developed by the US National Institute of Standards and Technology (NIST) to satisfy HSPD-12, a Homeland Security Presidential directive issued in 2004 stating that the US must establish "a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees)".

HSPD-12 further specified secure and reliable identification that is based on sound criteria for verifying an individual employee's identity, is strongly resistant to identity fraud, tampering, counterfeiting and terrorist exploitation, and can be rapidly authenticated electronically. This meant that all federal agencies had to put into place rigorous identity management practices, and that issued credentials had to be interoperable between federal agencies.

To achieve this, all applicants must go through an enrollment and identity verification process. The first stage is sponsorship, where the application process must be started by a known individual. Then comes registration, when an applicant's details such as their photo, fingerprints and supporting documentation are captured. The next step is adjudication, where a person's identity is confirmed via fingerprints and external agency checks. Only when an applicant's identity is assured can a PIV card be issued to them.

A PIV card acts as a single secure portable credential, effectively allowing the authenticated cardholder to log on to computers, access buildings and prove their identity as and when required.

How can PIV help my organization?

PIV offers a proven set of identity assurance best practices. When combined with a secure interoperable PIV card these provide an excellent benchmark for any organization wishing to enhance its security. For those who do business with federal organizations it shows a willingness to adopt complementary policies. For corporations it avoids 'reinventing the wheel' and allows lessons learned from federal government to be applied to other industry sectors.

A FIPS 201 compliant solution must use components that have been tested by NIST and placed on the Approved Product List (APL). This provides organizations with a 'shopping list' of proven interoperable components that are known to meet the highest security standards.

By following a PIV process, a chain of trust is established from the applicant's identity through to the issued credential. This enables organizations to be sure that all information on a PIV card has been gathered, checked and entered correctly and belongs to the person presenting the card.

Multiple mobile platforms

With your existing Cloud services

Using the latest mobile phone security features

For federal agencies…

To get a PIV card you must provide two forms of identification from an approved list (e.g. passport, birth certificate, driver's license), a photograph, your fingerprints and biographic data as required (e.g. your address). An initial FBI/OPM background check is conducted before an application is approved. This is followed by a NACI (National Agency Check with Inquiries), which can be completed up to six months after a card has been issued.

When an application is approved a trusted credential from a PKI can be issued on a device using an electronic personalization product. All of the components in this process must be on the GSA Approved Product List, which only includes products that comply with the FIPS 201 standard.

Intercede® MyID was the first identity and credential management solution to be placed on the Approved Product List and satisfies all of the criteria for a complete FIPS 201 compliant PIV process.

Intercede MyID PIV deployments at 14 federal agencies include: Federal Aviation Administration, Environmental Protection Agency, Social Security Administration and Nuclear Regulatory Commission.

For organizations who need PIV-interoperability…

A PIV-I card is a Personal Identity Verification Interoperable card. This means that it meets the technical specifications to work with PIV infrastructure and is issued in a manner that is trusted by Federal Government. A PIV-I card still includes biometrics (although fingerprints are not subject to the same rigorous background checks as for a full PIV card) and four PKI certificates.

PIV-I still strongly authenticates individuals, but a full NACI is not mandatory, and cards contain different identifiers on their signing certificates to those on PIV cards. Graphically, a PIV-I card must look different to a PIV card.

By using federated PIV-I credentials, non-governmental organizations can ensure interoperability when doing business with government departments and agencies. Industries such as aerospace, defense and transportation, which already operate globally, are now beginning to adopt PIV-I.

FIPS 201 leverages existing ANSI, ISO, IETF and other standards. For this reason thousands of products including most operating systems, mobile and enterprise applications and services and physical access control systems support PIV-I credentials.

Intercede MyID PIV-I deployments include: Booz Allen Hamilton and ORC, who operate MyID on behalf of a range of organizations including emergency first responders.

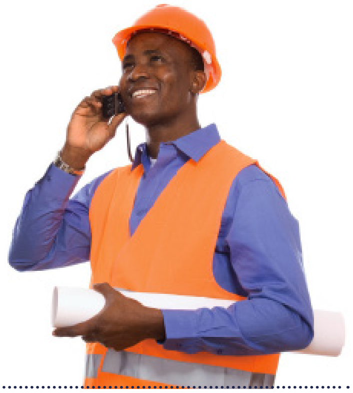
For corporations who want to follow best practice…

A CIV card is a Commercial Identity Verification card, also known as a PIV-compatible card. This means that it meets the PIV specifications, technology requirements and data model without the need for cross-certification and can therefore be issued by any enterprise. CIV cards are used by organizations that don't need to authenticate themselves to government agencies, but still want to benefit from features such as physical and logical access convergence, establish a single sign-on policy or get away from multiple passwords and/or cards per user.

Establishing a central identity management solution means that employees can be issued a single credential that they can use corporation-wide rather than having multiple identities for different resources and locations. This allows for simple or automatic revocation of access should an employee leave the company.

Using standards-based proven interoperable technology means that employees can use their CIV cards to do things like log on to Windows 7 immediately, without the need for middleware. Strong card authentication using cryptographic functions guarantees that a CIV card is authentic and can therefore be trusted, and the CIV process provides an organization with enhanced security, improved data protection, more secure networks and physical facilities, increased cost savings and improved efficiency.

Intercede MyID CIV deployments include: TWIC, Boeing and Lockheed Martin.



@ info@intercede.com   www.intercede.com   intercedemyid
Suite 920, 1875 Explorer Street, Reston, VA 20190, USA   +1 888 646 6943
intercede