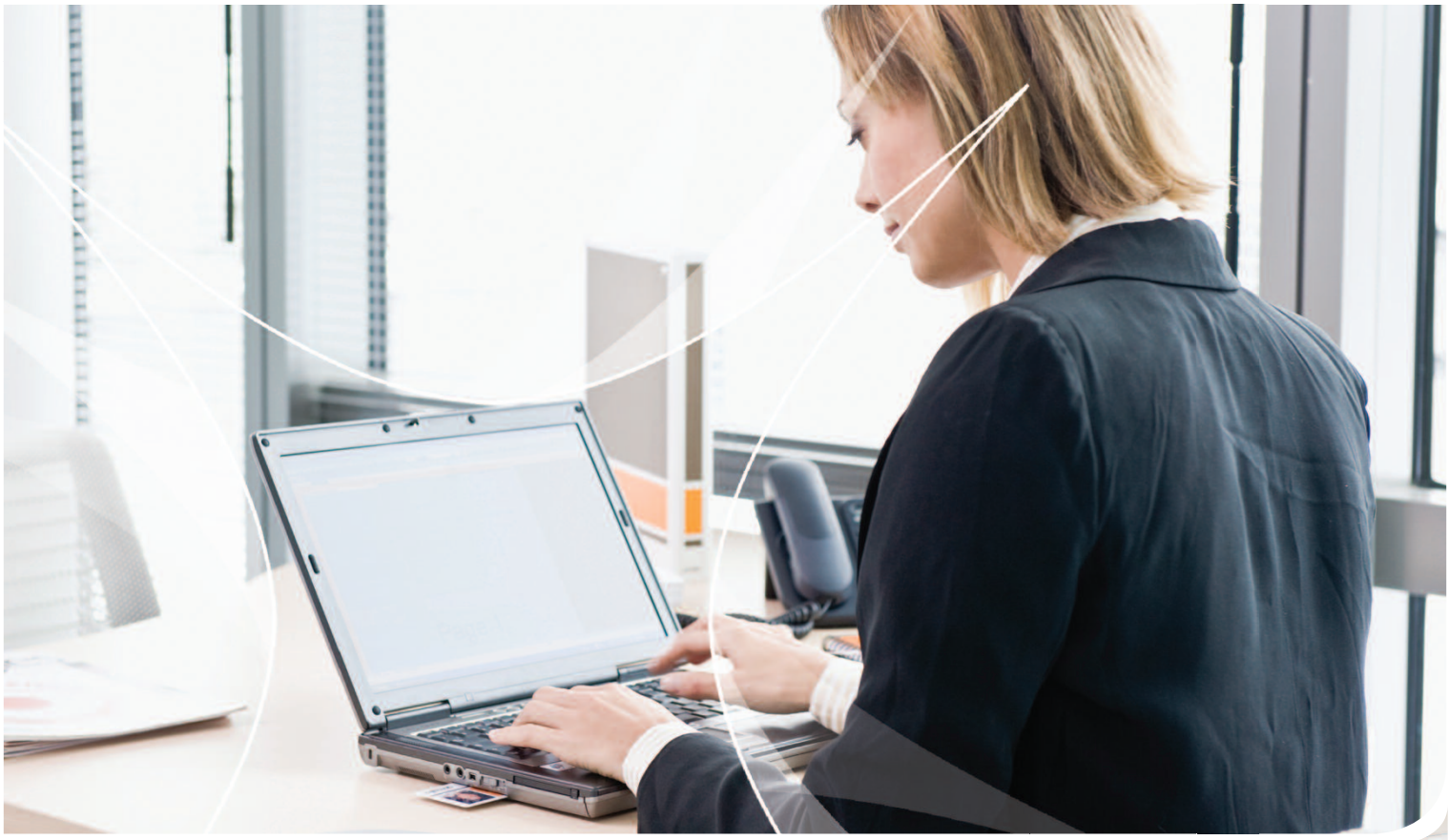
# Protiva™ PIV Cards and Solutions

Personal and Corporate Identity Verification-Interoperable ID Credentials for Private Sector, Government Suppliers, State and Local Governments



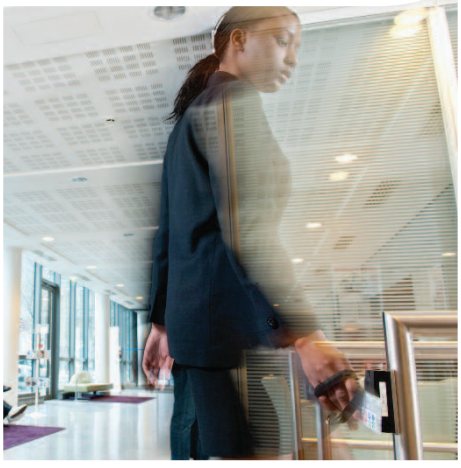
FINANCIAL SERVICES & RETAIL

ENTERPRISE

GOVERNMENT > SOLUTION

TELECOMMUNICATIONS

TRANSPORT



gemalto
security to be free

# Protiva PIV Cards comply with the Federal PIV technical specifications required for use as PIV-I and CIV Cards

Provides private sector, state and local government organizations with identity cards that can be trusted and interoperable with the Federal government.

Gemalto's Protiva PIV (Personal Identity Verification) Card is a standards-based card for private sector, state and local government organizations to issue credentials that the federal government can trust. The same card can be used for either a CIV or PIV-I based deployment depending on use requirements and infrastructure. Protiva PIV Cards deliver high levels of security for identity management and authentication, as well as interoperability and trust with federal agencies and departments.

## Uses of PIV

- Provides strong proof of cardholder identity that meets federal standards
- Digitally authenticates identity for information system and enables physical access
- Identifies users for physical access
- Digitally signs and encrypts eDocuments, email and files
- Works with federal government PIV-based IT infrastructures, and new and legacy physical access control systems
- Biometric fingerprint and iris delivers highest level of identity assurance

## PIV Technology and Standards

PIV card technology features a dual interface microprocessor chip for use with contact and contactless smart card readers, making it easily adaptable for a wide range of use cases. For compatiblity with legacy physical access readers based on Mifare and other technologies, Protiva PIV Cards are available with a tri-interface option. Protiva PIV Cards are certified Federal Information Processing Standard 201 (FIPS 201) and FIPS 140-2 Level 2 validated.

## PIV and the U.S. Federal Government

Most federal government employees and subcontractors have a PIV card. Driven by the issuance of Homeland


Security Presidential Directive 12 (HSPD-12) in 2004, the U.S. federal government has invested significant effort and resources in implementing robust, interoperable credentialing processes and technologies. The resulting standard, FIPS 201, Personal Identity Verification (PIV) for Federal Employees and Contractors, provides a framework of the policies, processes, and technology required to establish a strong, comprehensive identity credentialing program.

## PIV-I —Trusted and Interoperable

The goal of the PIV-I initiative is to widen the availability of identity cards that are able to interoperate with the federal government PIV systems and contain credentials that can be trusted by federal agencies. Organizations that issue PIV-I credentials must follow strict identity vetting guidelines including in-person proofing, two identity source documents and other requirements. This enables federal agencies and departments to trust PIV-I credentials and identities. Since PIV-I leverages federal standards and established best practices, PIV-I credentials and IT access systems are interoperable with federal PIV-based systems.

## Government Contractors and Critical Infrastructure Organizations

Implementing PIV-I identity credentialing and security systems helps enterprises, including those involved with the nation's critical infrastructure, to significantly upgrade the security of their information systems and networks. In addition, the fact that PIV-I credentials are trusted and interoperable with the federal government makes it much more efficient and secure for contractors to exchange information securely with their government clients. It also creates opportunities to improve business processes, such as digitally signing and encrypting contracts or specifications.

**Gemalto provides a comprehensive suite of solutions to implement the PIV/CIV standard for "something you have" network access and identity credentialing. It is specifically designed as a federated trusted identity credential for private sector government suppliers, critical infrastructure companies, and state and local governments.**

## State and Local Government

State and local governments can leverage the federal PIV program by using PIV-I as the basis for their identity credentialing and information system security. Many point to the PIV standard as a way to achieve a more

holistic approach to issuing identity credentials and improving their own business processes and information systems security. More than 16 states are currently planning or implementing some form of PIV-I or CIV (Commercial Identity Verification) strategy. PIV-I credentials are being used in regional and national interoperability exercises sponsored by the Federal Emergency Management Agency (FEMA) for First Responder Access Cards (FRAC). These credentials, typically issued by state and local governments, identify emergency responders for secure access to remote networks to pilot operations and access to Federal systems.

## Corporate Identity Verification Card

Corporations now have the ability to apply the security standards implemented by the U.S. federal Government to secure their networks and sensitive data based on PIV. By implementing identity verification procedures and issuing corresponding CIV cards for corporate identity, companies are implementing the same level of strong authentication already proven to be effective in protecting U.S. Military networks.

## Healthcare

The majority of healthcare systems use weak username and password single factor authentication that puts patient privacy and security at risk. Using PIV-I and CIV identity credentials can enable the healthcare industry to improve their information systems security, control who has access to which pieces of information. The credentials comply with HIPAA mandates for protecting individuals' privacy, and the DEA's Controlled Substances Act (CSA).

## Gemalto PIV Solutions

Gemalto's complete range of PIV solutions, including certified cards and readers, credential personalization and issuance systems, off-premise hosting, personalization, issuance and fulfillment services, and consulting provides these benefits:

- Improve security and efficiency when working with the federal government
- "Something you have" authentication provides protection from unauthorized access to information systems and networks
- Provides audit trail of individual access activity
- Easier and more convenient for employees than multiple, complex and changing passwords
- Easy to deploy for the administrator
- Thousands of Windows and MacOS IT infrastructure products support PIV-I credentials, making it easy to implement
- Proven performance based on federal standards
- Availability of complete turnkey PIV-I solutions with Gemalto simplifies deployment
- Secure, long-lasting card body uses security features such as holograms, UV rainbow printing, and Optical Variable Ink (OVI)
- Option for off-premise credential issuing and authentication server from Gemalto or a partner

## Technical Specifications

**General Features:**

- FIPS 201 Compliant™ supporting mandatory and optional data objects through SP 800-73-3, and FIPS 140-2 Level 2 validated.
- Customized PIV Admin Key set to a fixed value or diversified value by using Key Management Service (KMS)
- Customized PIN and Global PIN value, length and retry counter
- Secured data personalization through GlobalPlatform (GP) Secure Channel Protocol
- Extendable PIV data model to create additional data containers with their own access control rules
- Java Card Virtual Machine, RTE and API compliant with JC2.2.1
- Card Management & API compliant with:
  - GP 2.1.1 for SCP01 and SCP02 supported with scripting capability of Amendment A
  - GP 2.2 for SCP03 according to GP 2.2 Amendment Cryptographic algorithms:
  - Symmetric: 3DES (ECB, CBC), AES (128, 192, 256)
  - RSA: up to 2048-bit
  - HASH:SHA-1, SHA-256, SHA-384, SHA-512
- On-board cryptographic co-processor
- On-board RSA key pair generation
- PK-based Directory Access Protocol (DAP) to better control permissions for applets loaded on the card
- Delegated Management, allowing pre-authorized card content management performed by an approved application provider
- Multiple Logical Channels to allow selection of multiple applets at the same time
- Contact Interface:
  - Protocols: T=0, T=1, PPS
  - Baud rates up to 230Kbps
- Contactless Interface:
  - ISO14443 type
  - A & B communication mode
  - T=CL supported with speed up to 848 Kbps
- Proximity Interface:
  - Mifare-1 (standard Key A or Key B) emulation
  - HID Prox (125 kHz) compatibility option

**Infrastructure Support**

- Integrated with card management systems (CMS) from HID, Intercede and more
- Works with all PIV compliant middleware

**Performance**

The Protiva PIV-I Card's Virtual Machine has been highly optimized to offer maximum software performance without compromising security. Combined with the high performance of the latest generation semiconductor technology, this makes the card one of the fastest Java Open platforms available.

**Security**

The Protiva PIV-I Card includes multiple hardware and software countermeasures against state-of-the-art attacks, including:

- Side channel attacks
- Invasive attacks
- Advanced fault attacks
- Timing attacks
- Fault attacks
- Card tearing
- Differential power analysis
- Simple power analysis
- Electromagnetic analysis

**More information about the Protiva PIV Cards is available at:**
www.gemalto.com/products/piv_card
**Information on the TOP Java Cards is available at:**
www.gemalto.com/products/top_javacard

## Contact Us

Gemalto, Inc.
Arboretum Plaza II
9442 Capital of Texas Highway North,
Suite 400
Austin, TX 78759-7262

Toll-free: 877-291-1312

www.gemalto.com/php/contactus.php


The world leader in digital security

www.gemalto.com



gemalto
security to be free