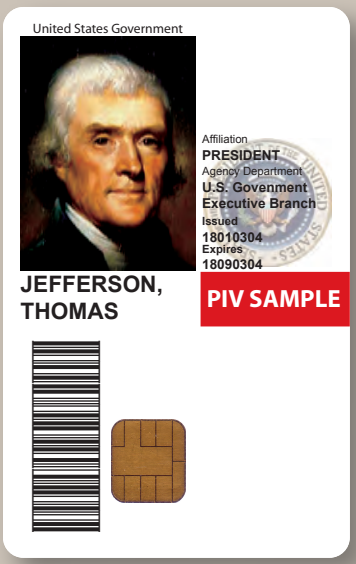
PIV Smart Card

Credentsys-J™ Dual Interface FIPS 201



For secure identity and access, the CardLogix FIPS 201 certified smart card meets the highest security standards for U.S. Government and business. The card provides instant, portable authentication for access to facilities and networks as well as digital signature, encryption, and other features and services. With dual interface capability, the card can be used with a wide range of access points and readers. The card is certified to comply with ISO 7816 and ISO 14443 standards for contact and contactless smart cards.

Featuring a patented Flexible Bump technology, the FIPS 201 card is durable and securely tested for ruggedness. Multiple secure printing options such as ultraviolet inks, microprinting, and guilloches can make the card highly resistant to duplication and fraud.

CardLogix, a leader in secure identity smart cards, is trusted to deliver the optimum in smart card technology and design support for government, business, and people worldwide.

IDENTITY

CardLogix PIV Card Highlights

Fully Approved for U.S. Government Applications

After rigorous, independent testing, the CardLogix Credentsys-J™ FIPS 201 card is completely certified for security and durability by certified NIST laboratories (FIPS Certificate No. 9 for FIPS 201 and Certificate No. 917 for FIPS 140-2). The requirements for certification stem from the PIV II Homeland Security Presidential Directive 12 for government agencies and their suppliers. The card also carries EAL 5+ certifications for the semiconductor used.

Flexible and Modular

The card enables virtually endless system expansion with open architecture and GlobalPlatform 2.1.1 specifications for post-issuance loading of applets. Interoperability via compliance with Java Card specifications supports applets from most third party vendors. In addition, custom applications can be developed independently from the card platform.

Dual Interface

With dual interface, not only are there more options for access and readers, but deployments can be mixed, according to required security and available resources.

Optimized Card Life – Extended Memory Support For Data and Applications

With 72k Bytes of user EEPROM, data storage and hosting of additional applets is not a problem. With the card's open architecture and an onboard applet, the creation of custom data models is easy.

CardLogix
16 Hughes, Suite 100, Irvine, CA 92618 USA
Phone +1 949 380-1312 · Fax +1 949 380-1428 · www.cardlogix.com · sales@cardlogix.com

PIV Smart Card

Credentsys-J™ Dual Interface FIPS 201

Secure Personalization

Cards support operations for loading cardholder-specific information via Secure Channel Operations, as specified by GlobalPlatform requirements. Safe, streamlined integration with most issuance systems is effortless, and proper security mechanisms used to load user credentials is assured.

On-Card Application Development

The most advanced applications are supported, ensuring return on investment. In addition to HSPD-12, Java Card, and GlobalPlatform specifications, the card supports garbage collection, multiple logical channels, and Security Domain extradition.

A Key Part of A Complete Smart Card Platform

The CardLogix FIPS 201 smart card is part of a platform that includes development and operating system software, as well as applets, readers, and graphic printing options. CardLogix combines all these resources to provide true end-to-end secure identity solutions.

Features

- 72k Bytes of user EEPROM
- Credentsys-J™ supports many of the upcoming NSA Suite B algorithms
- 32-bit RISC processor cores with DES, AES and PKI Crypto acceleration
- Crypto library utliizing hardware crypto accelerators for 3DES, AES, RSA up to 2048 bits, and Digital Signature Algorithmic operations
- Full implementation of the logical credential data model including PIV II, Card Holder Unique ID, and PIV Authentication. All optional containers are supported.
- Individual authentication via PIN or biometrics
- Full support for high-level PIV client APIs and low level interface commands at card edge
- Built-in PIV II Card Application with CHUID data object. Post-issuance applications can be loaded as required.
- Fully interoperable within any PIV II environment

Dedicated Hardware and Software Countermeasures Guard Against:

- Side channel attacks
- Advanced fault attacks
- Velocity checking
- Voltage attacks
- Frequency attacks
- Temperature glitch attacks
- Optical attacks

Secure Printing Options include:

- Laser Engraving/Indenting
- Guilloche and Rosettes
- Microprinting
- Optical Variable Devices (OVDs)/Holograms
- Hidden Card Validator™ graphics with lens viewer
- Ultraviolet (UV) Ink

Memory Management

- Applet deletion
- Real garbage collector (JC 2.2.1 specification)
- Secure memory management/access protection (Supervisor Mode)