



PIV-Based Smart Credentials

PKI credentials for commercial use



GOVERNMENT STANDARDS AREN'T JUST FOR GOVERNMENT.

For almost two decades, IDEMIA has been the leading supplier of PIV and CAC cards to the U.S. federal government.

The IDEMIA ID-ONE CIV® (Commercial Identity Verification) smart card is based on the PIV solution, making government-grade security available to the commercial sector for physical and logical access control. In this commercial application, the card allows private keys and certificates to be updated on the card after PIN verification, thus allowing PKI smart card creation without a CMS (Credential Management System), while still complying with all required and optional features of NIST's FIPS 201 and SP-800-73-4 standards.

As the market leader, IDEMIA's PIV/CIV solution is supported by all major CMSes. Cards can be graphically personalized and mailed centrally from IDEMIA's U.S.-based manufacturing, personalization, and fulfillment facilities, or managed by CMS personalization at customer locations.

KEY FEATURES

- Fully compliant with all federal standards.
- Longstanding track record of providing secure credentials to customers with the highest security requirements.
- Long-term commitment to the PIV market, with newer models responding to future trends in cryptographic and security standards.

Key Benefits

INTEGRATED PAC AND LAC SOLUTION

One smart card for physical and logical uses, both contact and contactless.

STANDARDS-BASED AND INTEROPERABLE

U.S. government standardized solution; not vendor-proprietary.

VERSATILE AND CONFIGURABLE

Flexible solution based on customer needs.





LOGICAL ACCESS

Can be used for Windows smart card login, email signing and encryption/decryption, secure website access, single sign-on, and VPN.

PHYSICAL ACCESS

Any PACS/reader system that supports PIV access control can be used, thus providing a one-card solution. Biometric access can also be added, as the card offers a PIN-protected cardholder fingerprint, and the option of on-card fingerprint matching.

PHISHING-RESISTANT

The PKI-based solution uses cryptographic authentication with on-card keys, providing a more secure solution than KBA (Knowledge-Based Authentication).

ADDITIONAL OPTIONAL FEATURES

- The Dual Hybrid adds a 125 kHz proximity chip for non-federal customers who need it to support existing physical access control reader infrastructure.
- The Secure PIN Entry (SPE) version has FIPS-140-2 certificate #3864 to achieve overall Level 3, and is supported by the IDEMIA mini-driver.
- A FIDO2 applet may be added if desired.
- A DESFire™ contactless chip can be added to support existing door reader infrastructure.

