Entrust®
Securing Digital Identities & Information

EntrustSecurity
@Entrust

Strong Identity Authentication for First Responders

Entrust Solutions for Compliance to U.S. Department of Homeland Security First Responder Authentication Credential (FRAC) Standards

Entrust.com
1-888-690-2424
Entrust@Entrust.com

Entrust®
Securing Digital Identities & Information

Table of Contents

FRAC Authentication Requirements

As stated by the U.S. Department of Homeland Security, “Local and state emergency response officials must be able to collaborate to ensure public safety. However, for this to happen, many identity management challenges must be overcome.

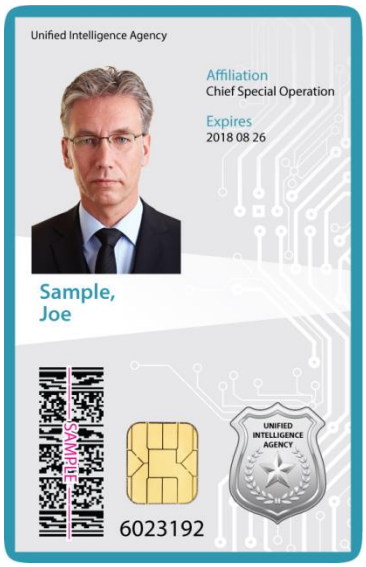
While federal agencies are rapidly deploying secure common identification standards based on guidance from the White House and other federal entities, state and local emergency response officials are working to establish a Personal Identity Verification-Interoperable (PIV-I) and First Responder Authentication Credential (FRAC) standard that is interoperable between local, state and federal levels.

In the past, physical access to sites would be granted based on personal judgment, rather than on hard identity data. Logical access to computer systems required only a username and password.

Today, Federal Information Processing Standard (FIPS) 201, Office of Management and Budget (OMB) memorandum M-05-24 and other White House guidance specify that access to all federal computer systems requires secure forms of identification based on smart card technology and identity-proofing procedures.”

The PIV-I Credential

Entrust provides PIV-I smartcard issuance solutions that are based on the FIPS-201 standard. The solution enables first responders to comply with the FRAC initiative while simultaneously meeting their own internal business needs — all in an economical, quick-to-deploy manner.



The Entrust solution provides all necessary authentication capabilities for FRAC, plus the ability to use the credential elsewhere within an organization. This proven approach provides a digital certificate from Entrust's certification authority (CA) service, stored on a FIPS-140 level 2 smartcard, with printed graphics that comply to the PIV-I federal standard.

In addition, the smartcard chip also contains a facial image and two fingerprints, which are digitally signed to prevent modifications.

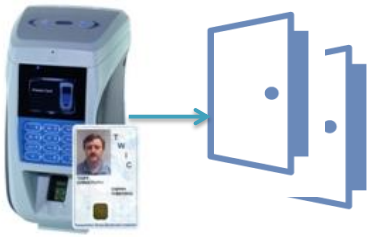
After the card is issued, the process of distributing the first responder credential involves identity-proofing:

- Visual confirmation of an employee's identity using a government-issued document
- Comparison of the fingerprints on the smartcard to the employee's fingerprints before either the card or PIN are issued

Authenticating PIV-I Credentials

The intent of the PIV-I credential is to provide a digital identity for secure physical and logical access that cannot be copied, plus a high degree of certainty it is being operated by the owner.

Authentication at the scene of a disaster requires the first responder to present their card to a FIPS-201-compliant handheld reader. The reader allows for the check of the PIN, facial image stored on the chip and the fingerprint stored on the chip.



The credential may also be used for physical access. The PIV-I (FIPS-201) standard supports four types of authentication, with the most secure being a mix of PKI and fingerprints. The PIV-I card also may be accepted for physical access by visitors to federal facilities.

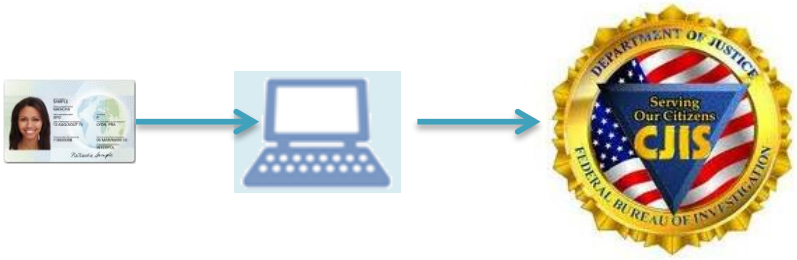
Leveraging FRAC Credentials for CJIS Compliance

The Criminal Justice Information System (CJIS) provides state, local and federal law enforcement with access to critical personal information such as fingerprint records, criminal histories and sex offender registrations.

In order to prevent unauthorized access to this extremely sensitive information, a security policy governing the access to the CJIS database was enacted on January 1, 2011.

CJIS compliance information was set in a mandate released by the FBI. The mandate sets forth the minimum requirements for securing access to the data included within CJIS.

The policy requires advanced authentication to be implemented across all those that agencies that access the information contained in the CJIS database.



The FRAC credential is an excellent method to meet CJIS compliance while reducing the number of credentials to carry. For more information about CJIS, visit **entrust.com/CJIS**.

One Platform for All Authentication Needs

In addition to issuing FRAC credentials, the Entrust solution provides many other authenticators from a single platform. The enterprise can deploy different authenticators to different employees to maximize the value of their investment.

Rather than deploying a one-time-passcode (OTP) solution to achieve assurance for CJIS-compliant remote access, and another solution to issue and manage PIV-I smartcards, organization may purchase, install and operate just one platform.

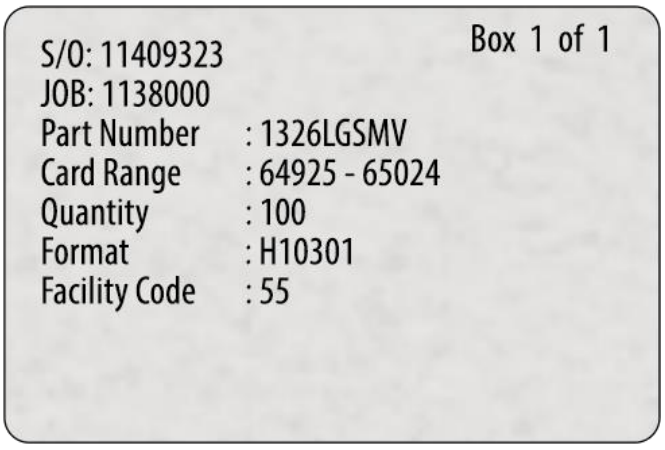
Secure Physical Access Systems

In addition to the functionality required for FRAC, the solution also may be used for both physical and logical access within the enterprise.

For pre-FIPS-201 physical access systems, the Entrust smart credential incorporates a second chip that can emulate a wide variety of physical access systems using Entrust IdentityGuard.

By incorporating both technologies in a single credential, the enterprise may move from older compromised physical access systems to newer more secure systems at their own pace, or only for high-value facilities without the need to change employee behavior.

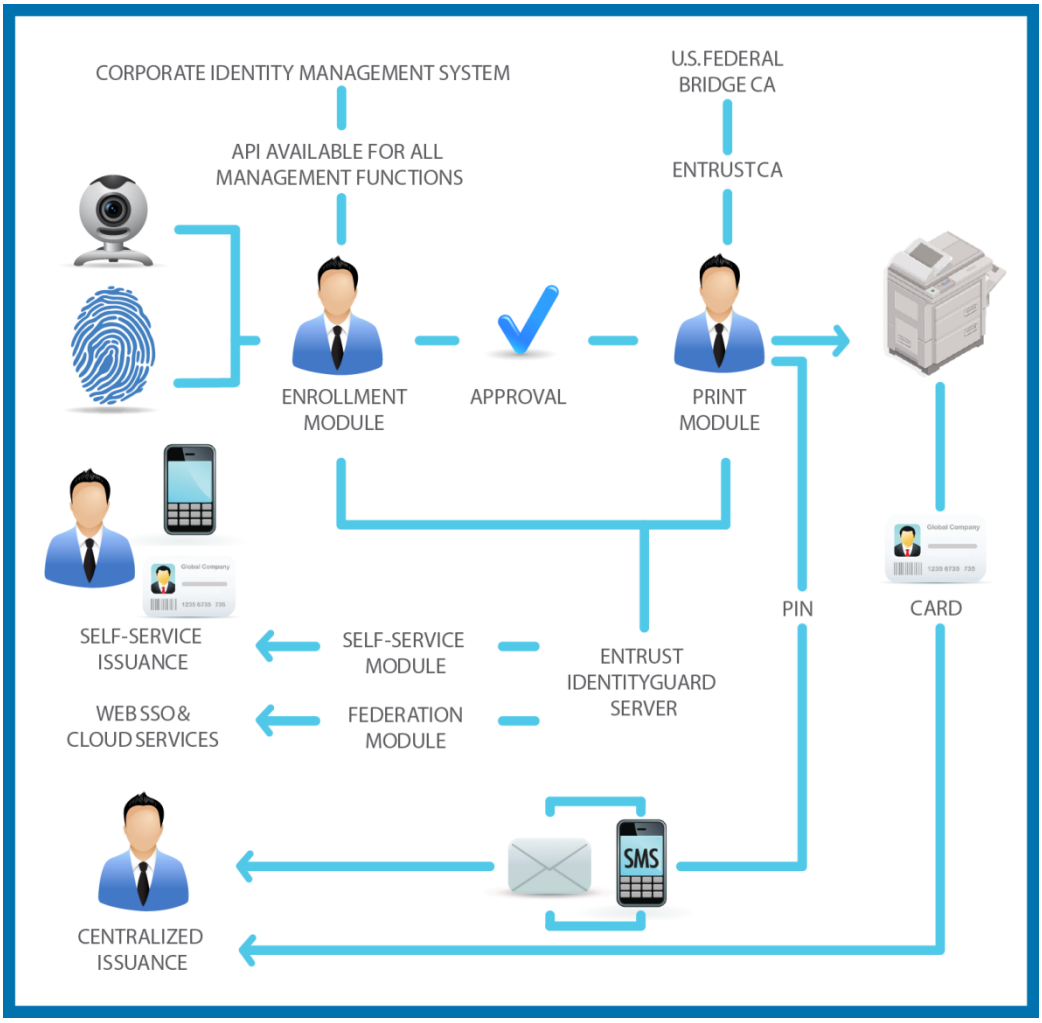
To confirm the support of your physical access system, Entrust requires the part number, format and facility code of your current physical access system found on the box your cards came in (see example below).



End-to-End PIV-I Credential Issuance

Entrust provides a turn-key, easy-to-deploy solution to comply with FRAC authentication requirements. This solution both issues and authenticates the credentials — all from a single platform.

Offered as a fully hosted PKI, Entrust Managed Services PKI is cross-certified to the Federal Bridge CA. This certificate service is accessed via Entrust IdentityGuard, so there's no need for the enterprise to set up and manage a CA.



Out-of-the-Box Modules

Entrust IdentityGuard also incorporates several modules:

Server Module — Often deployed as a pair for active-active high availability. This module also incorporates a credential issuance workflow, which allows the enterprise to control the process and provide approval logs for future audits. All user interfaces can also be invoked through an API by your existing identity management system. The enterprise has the choice of deploying a new repository for credential data, or reusing an existing repository to reduce the total cost of ownership. The credential data can be encrypted in the existing repository for confidentiality reasons.

Self-Service Module — Allows users to reset or change their own PIN, or issue/renew their own credentials. Issue temporary or replacement credentials so the employees can continue to work in the event their primary credential is unavailable.

Print Module — Sends smartcard print jobs to the printer; when the printer is equipped with a "smartcard encoder" the chip also may be encoded with digital certificates and biometrics. Please note that there is one print module per printer; recommended printers are the HDP5000 and SR300 with their associated smartcard encoder.

Enrollment Module — Used to enroll employees for the items below. There is one enrollment module for each enrollment station within an organization (often depends on the number of physical locations). Entrust suggests the module be deployed where you currently take employee pictures for physical access cards.

- ***Pictures:*** Web Cam, such as the Microsoft LifeCam HD3000, or a Datacard Secure Capture device, which will automatically adjust flash and crop the picture.
- ***Fingerprint:*** When PIV-I is utilized, a FIPS-201-compliant fingerprint scanner must be used, such as the Futronic FS-88 or Cogent CSD-200.
- ***Signature Pad:*** This is not required for PIV-I, but may be used for any of the cards. The signature may be printed on the cards.

Federation Module (Optional) — Deployed in front of a cloud service's SAML Service Point, such as Salesforce, or in front of a Web single sign-on product to add a strong, single authenticator to meet all your needs.

Unique Deployment Options

Entrust IdentityGuard may be deployed in two methods, combinations not available from any other vendor.

Deployed within the Enterprise — Allows the enterprise to enroll employees and print both new and replacement cards on their own premises using the certification authority (CA) located at the Entrust facility.

Deployed via the Cloud — Gain the benefits of a software authentication platform but offered as a cloud-based service. Simply contact Entrust with the number of cards you need. Entrust prints and encodes the cards with certificates, then mails them to your offices worldwide.

Entrust IdentityGuard Credentials & Readers

Entrust offers all the necessary authenticators as required by the U.S. Department of Homeland Security for FRAC.

FIPS-140 Level 2 Smartcards or USBs

Unlike the competition, the Entrust smartcard utilizes a new technology where the contactless antenna is not directly connected to the chip. This allows the card to last up to 10 years; competitor cards will fail as soon as 2 years from constant stress and flexing (e.g., stored in a wallet), which detaches the antenna from the chip.

Due to federal policy, only a card-based form factor can be used with PIV-I. However, the same platform can be used for the USB form factor for non-PIV-I applications.

Mobile Smart Credential

Taking advantage of near-field communication (NFC) and Bluetooth standards, Entrust mobile smart credentials embed digital certificates on smartphones to create trusted identity credentials for stronger, more convenient enterprise authentication to desktop/laptop computers and physical access.

These same credentials may also be used within smartphones for authentication to mobile applications such as a Web browser or SMIME email client.

Always on hand, these multipurpose credentials securely access computer workstations, network resources, data, cloud applications, physical doors or buildings, and also enable users to digitally sign transactions and encrypt data.

Critical corporate transactions and forms may be sent effortlessly and securely to the mobile device for digital signatures using a Wi-Fi or cellular connection.

One-Time Passcodes

Entrust offers one-time passcodes (OTP) in both a plastic form factor or as a mobile application. While not suitable as a FRAC credential, the organization may find these suitable for use within the organization as a valuable low-cost authenticator.

Smart Card Middleware

The Entrust smartcard is supported by Windows 7 and 8 without installing a driver. In the cases where Windows XP or Vista is used, Entrust provides Entrust Security Provider. ESP has the additional value of:

- Supports a secure PIN entry device where the PIN is not entered by the Windows keyboard, so the PIN cannot be stolen by Windows keylogger malware.
- Right-click file encryption using the encryption keys on the smartcard. The files can only be decrypted when the smartcard is present in the computer and the PIN is entered. This eliminates the risk of malware stealing files that are in plain text.

Smartcard Readers

Entrust supplies a variety of readers:

- Contact card readers
- Contactless card readers
- Secure PIN entry contact card reader
- Card readers built into laptops

Hardware Security Module

To protect card management and certificate issuance keys from theft from malware or employees, the keys used by Entrust IdentityGuard must be stored in a Hardware Security Module, which Entrust will provide on request.

Platform Features

The First Responder Authentication Credential, based on the PIV-I standard, can also be used for authentication within your organization:

- Authentication to full-disk decryption for products that support the PIV standard
- Authentication to Windows/Mac/Linux login with multiple credentials for administrators; eliminates need for employees to reset forgotten passwords or change passwords every 90 days
- Authentication to VPN access
- Authentication to Web single-sign on (SSO)
- Authentication to any Web application (e.g., Outlook Web Access) that uses client-side SS
- Enables transparent file encryption
- Offers email encryption and digital signing within Microsoft Outlook; emails signed by these certificates are publicly trusted, so recipients outside your enterprise or within the federal government will trust the signature

The Entrust IdentityGuard Platform also issues device certificates for both Windows and mobile devices that need to connect to the corporate network. This helps protect the network from improper device access while eliminating the need for the user to enter a username and password.

Future PIV-I Solutions

Entrust is committed to providing solutions that solve the business problems facing customers — now and in the future.

Entrust recognizes that customers need to access sensitive information systems from their mobile phone or tablet. The difficulty comes from trying to use the federally mandated PIV-I smartcard form factor with a mobile phone and tablet, which do not readily support these smartcards.

Entrust offers an innovative solution that embeds the same PIV-I application used within the smartcard into the mobile device. This provides the same strong authentication without the need to carry around a plastic card and card reader.

Before this can be used for FRAC, the U.S. federal government needs to complete changes to the standard under FIPS-201 Version 2.

Entrust is well underway in completing these changes and is in trial with leading federal agencies to bring this to the FRAC market as soon as possible.

In addition to being used within the mobile device to access email, websites and telephone communication during a disaster, the credential man also be used outside the mobile device to authenticate to third-party readers that are compliant to FIPS-201-2.

Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects,

Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

A trusted provider of identity-based security solutions, Entrust empowers governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL.

For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **entrust.com**.

Company Facts

Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 Globally

Headquarters

Three Lincoln Centre
5430 LBJ Freeway, Suite 1250
Dallas, Texas 75240

Sales

North America: 1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com

follow us on twitter