Entrust®
Securing Digital Identities
& Information

EntrustSecurity
@Entrust

Strong Authentication for Healthcare

Entrust Solutions for Centers for Medicare & Medicaid Services Authentication Compliance

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

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners.

The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional.

ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS O F THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

Table of Contents

CMS Authentication Requirements 4

End-to-End Token & Credential Management ... 8

Out-of-the-Box Modules 9

Unique Deployment Options............................ 11

Entrust IdentityGuard Credentials.................... 12

FIPS-140 Level 2 Smartcard or USB 12

Mobile Smart Credential.. 12

One-Time Passcodes (OTP) 13

Smart Card Middleware 13

Smartcard Readers 13

Hardware Security Module 13

Secure Physical Access Systems 14

Entrust IdentityGuard: Authentication, Encryption & Signature Capabilities 15

FIPS-201 Approved Products List 16

The Entrust Difference: One Platform, All Approved Authenticators.................................. 17

Entrust & You 18

CMS Authentication Requirements

In July 2012, the Centers for Medicare & Medicaid Services (CMS) issued the standard[1] for the use of multifactor authentication mechanisms in CMS systems.

As an expert in multifactor and identity authentication, Entrust provides capabilities to healthcare organizations that far surpass the regulations.

We work with many of the top healthcare organizations in the United States to ensure they meet the requirements set out to mitigate risk and the investment needed to fulfill their obligations.

Depending on the CMS system being accessed, employees require an overall authentication level from 2 to 4, with 4 allowing access to all CMS systems. The list of authenticators is outlined in the table on the following pages.

[1] "CMS Authentication Standards, Version 1.2," Centers for Medicare & Medicaid Services (CMS), July 31, 2012.

CMS Overall Assurance Requirements	U.S. Federal Assurance Level	Tokens	Identity-Proofing
2	**Not Applicable**	A single-factor, one-time-passcode (OTP) device. These devices, captured in Table 12 of page 48 of the CMS standards document, are suitable for infrequent users of the CMS systems.	From Table 8, page 33, of the CMS standards document: *Possession of a valid current primary government picture ID that contains Applicant's picture, and either address of record or nationality of record (e.g., driver's license or passport).*
3	**FBCA Basic**	A digital certificate that may be stored in Microsoft CAPI, a USB, smartcard or Entrust Mobile Smart Credential.	The employee receives the certificate after proving they are in possession of a physical address. Entrust IdentityGuard asks the employee questions with the answers in the employer's database to prove their identity. The credential or shared secret to obtain the soft credential is then mailed to the employee's physical address.

CMS Overall Assurance Requirements	U.S. Federal Assurance Level	Tokens	Identity-Proofing
3	**FBCA Medium**	A digital certificate that may be stored in Microsoft CAPI, a USB, smartcard or Entrust Mobile Smart Credential. Optionally, the employee's biometrics can be stored within the smartcard.	The enterprise places a number of employees into the role of Trusted Agents or, for an additional fee, Entrust will provide Trusted Agents. The Trusted Agent provides the employee (subscriber) their token/credential during a face-to-face meeting where the government-issued identity document (e.g., passport) is checked. The subscriber signs an agreement acknowledging the need to protect the credential from misuse, and to report when lost or stolen. The PIN is sent through an alternate channel to prevent misuse. Alternatively, for remote employees, the following are also allowed: ● A Notary will perform the face-to-face identity-proofing. ● US federal policy allows for online question-and- answer identity-proofing referencing an Antecedent event. An Antecedent event is an in-person proofing event that occurred previously, such as obtaining a driver license or loan. The questions would prove you had possession of the driver license or the loan.
4	**FBCA Medium Hardware**	This credential requires a digital certificate to be stored on a FIPS-140 level 2 smartcard, USB or Mobile Smart Credential. Optionally; the employee's biometrics can be also stored within the device.	

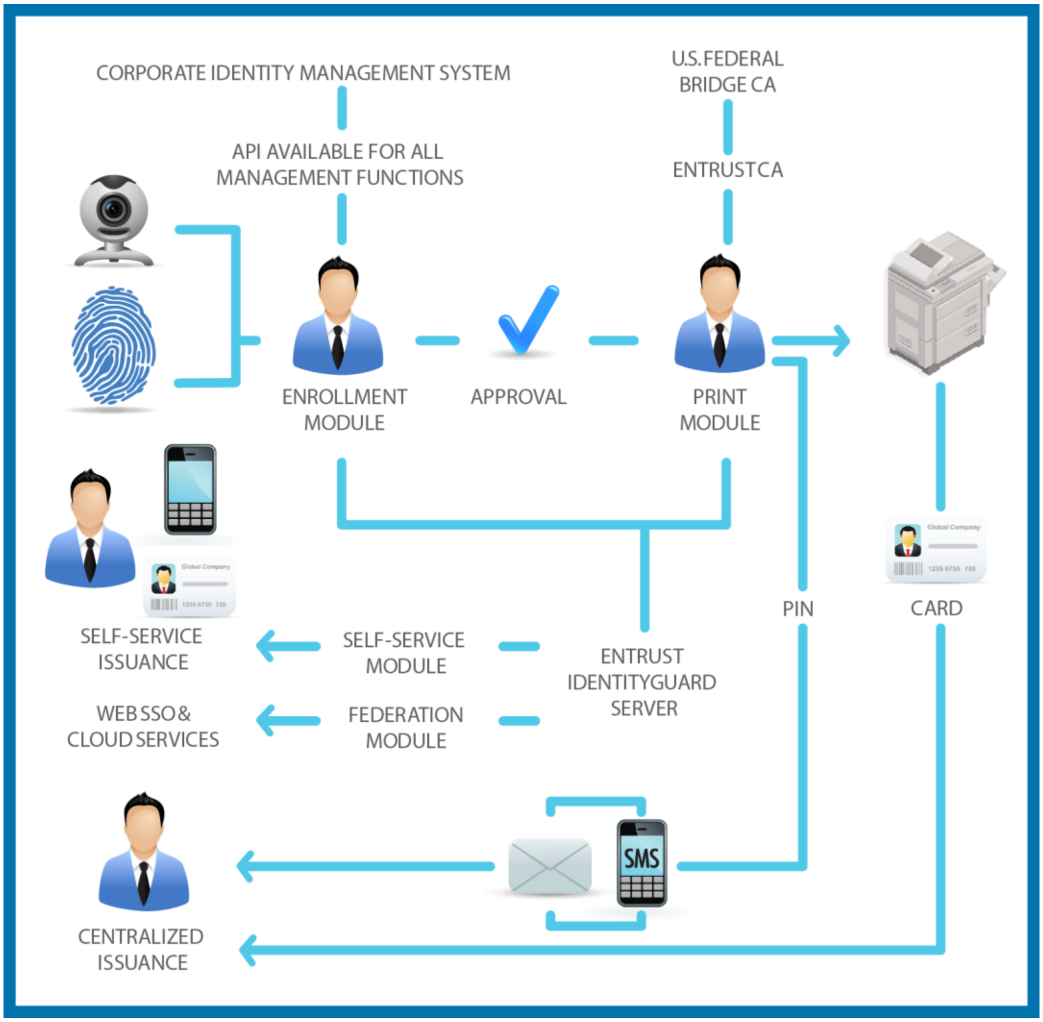
CMS Overall Assurance Requirements	U.S. Federal Assurance Level	Tokens	Identity-Proofing
4	FBCA PIV-I Auth	This credential requires a digital certificate to be stored on a FIPS-140 level 2 smartcard, with graphics restricted to specific regions on the face of the card. The smartcard chip must contain a digitally signed facial image and two fingerprints. It is digitally signed to prevent modification by a person attempting to create a fraudulent card. This credential is useful for physical access readers that use a fingerprint within an enterprise and for situations where the employee frequently visits a U.S. federal facility. The PIV-I card may be accepted for federal physical access. If the organization does not need fingerprint capabilities or physical access to federal buildings, consider FBCA Medium as it is also overall Level 4 without the added cost of capturing and storing employee fingerprints.	This is the same process as medium assurance, with the addition that the biometrics of the employee must be checked against what is stored on the credential prior to providing the credential and/or PIN.

End-to-End Token & Credential Management

Entrust is an industry expert in identity authentication. We know it’s not an easily managed activity for any organization and that’s why we provide a turn-key, easy-to-deploy solution to comply with CMS authentication requirements. This solution both issues and authenticates the credentials — all from a single platform.

Offered as a fully hosted certificate authority, the Entrust CA is cross-certified to the Federal Bridge CA. This certificate service is accessed via Entrust IdentityGuard, so there’s no need to set up and manage a certification authority.

Where desired, Entrust IdentityGuard can also simultaneously connect to your on-premise Microsoft CA for total control, permitted by all issuance, from one system.



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 be invoked through an API by existing identity management systems. 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 may be encrypted in the existing repository for confidentiality reasons.

Self-Service Module — Allows users to reset or change their PIN or issue/renew their credentials.

Print Module — Sends smartcard print jobs to the printer; when the printer is equipped with “smartcard encoder” the chip also may be encoded with digital certificates and biometrics.

The recommended printers are the HID HDP5000 and Datacard SR300 with their associated smartcard encoder.

For PIV-I credentials, the printer utilized for card issuance must be on the FIPS-201 Approved Products List under the category “card printer station.” The Entrust solution incorporates compliant products.

Enrollment Module — Used to enroll employees for the items below. There is one enrollment module for each enrollment station within an organization.

Entrust suggests the module be deployed where you currently take employee pictures for physical access cards.

- ***Pictures:*** A Web cam, such as the Microsoft LifeCam HD3000 or a Datacard Secure Capture device, 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.
- ***Signature Pad:*** This is not required by CMS but may be used for any of the cards. The signature would be printed on the cards.

Requirement for PIV-I credentials — The fingerprint scanner, the fingerprint template generator and camera must be on the FIPS-201 Approved Products List under the category “Single Fingerprint capture Device,” “Template Generator” and “Facial Image Capturing Camera.” The Entrust solution incorporates compliant products.

Federation Module (Optional) — This SAML-compliant Identity Provider is deployed in front of a cloud service, such as Salesforce, or in front of a Web single sign-on product to provide a strong, single authentication solution across the entire enterprise.

Unique Deployment Options

Entrust IdentityGuard may be deployed in three methods, which are not available from any other vendor. We will work with you to help choose the best option to meet your business needs.

1. **Deployed within Customer Premises**
   The organization enrolls employees and prints both new and replacement cards on-premise.

2. **Deployed via the Cloud**
   Gain the benefits of a software authentication platform but offered as a cloud-based service. Simply contact us with the number of cards you need. We print and encode the cards with certificates, then mail them to your offices worldwide.

3. **Hybrid**
   While the bulk of the solution is delivered by the Cloud, the Entrust Professional Services will bring additional enrollment stations and print stations to your facility for the initial enrollment of all employees, and then leave fewer enrollment and print stations at your facility for small volume new and replacement credentials.

Entrust IdentityGuard Credentials

While Entrust offers the solution as required by the Centers for Medicare & Medicaid Services, it also provides for all the enterprises authentication needs outside CMS compliance as described below.

FIPS-140 Level 2 Smartcard or USB

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 two 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.

Mobile Smart Credential

Taking advantage of near-field communication (NFC) and Bluetooth standards, Entrust mobile smart credentials embed digital certificates on smartphones to create a smart card like, trusted identity credential for stronger, more convenient enterprise authentication.

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 (OTP)

The OTP credential is offered in both a plastic form factor or as a mobile application.

Smart Card Middleware

The Entrust smartcard/USB is supported natively by Windows 7 and 8. In the cases where Windows XP or Vista is used, Entrust Security Provider provides the necessary driver and this additional value:

- Supports a secure PIN entry device where the PIN is not entered by the Windows keyboard, so the PIN cannot be stolen by Windows key logger 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 by malware or employees, the keys used by Entrust IdentityGuard must be stored in a Hardware Security Module, which Entrust will provide on request.

Secure Physical Access Systems

In addition to the functionality required for the Centers for Medicare and Medicaid, the solution also may be used for physical access within the enterprise:

- Physical access for both existing systems and newer FIPS-201 access systems.
- 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.
- In addition to issuing a combined physical and logical access credential, the Entrust solution will also notify your physical access system that the new credential has been issued or revoked.

  When integrated with your existing identity management system, and HR adds the employee to payroll, Entrust IdentityGuard will create the physical/logical credential and notify the physical access system. This saves time and effort versus performing these steps manually.

Entrust IdentityGuard: Authentication, Encryption & Signature Capabilities

- 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 SSL
- Issues device certificates for both Windows and mobile devices that need to connect to the corporate network; protects network from improper device access while eliminating the need for the user to enter a username and password
- Enables file encryption
- Offers email encryption and digital signing within Microsoft Outlook; emails signed by these certificates are publicly trusted, so recipients outside your enterprise, within the US Department of Health & Human Services DIRECT program or within the federal government will trust the signature

FIPS-201 Approved Products List

As mandated by the CMS policy, the Entrust solution uses components from the FIPS-201 Approved Product List:

- Electronic Personalization – Entrust IdentityGuard
- PIV Card – Entrust PIV Card
- Facial Image Capturing Camera
- Single Fingerprint Capture Device
- Template Generator

For PIV-I credential issuance, Entrust is an Approved PIV-I entity as described by the federal government. Reference http://www.idmanagement.gov/approved-piv-i-entities

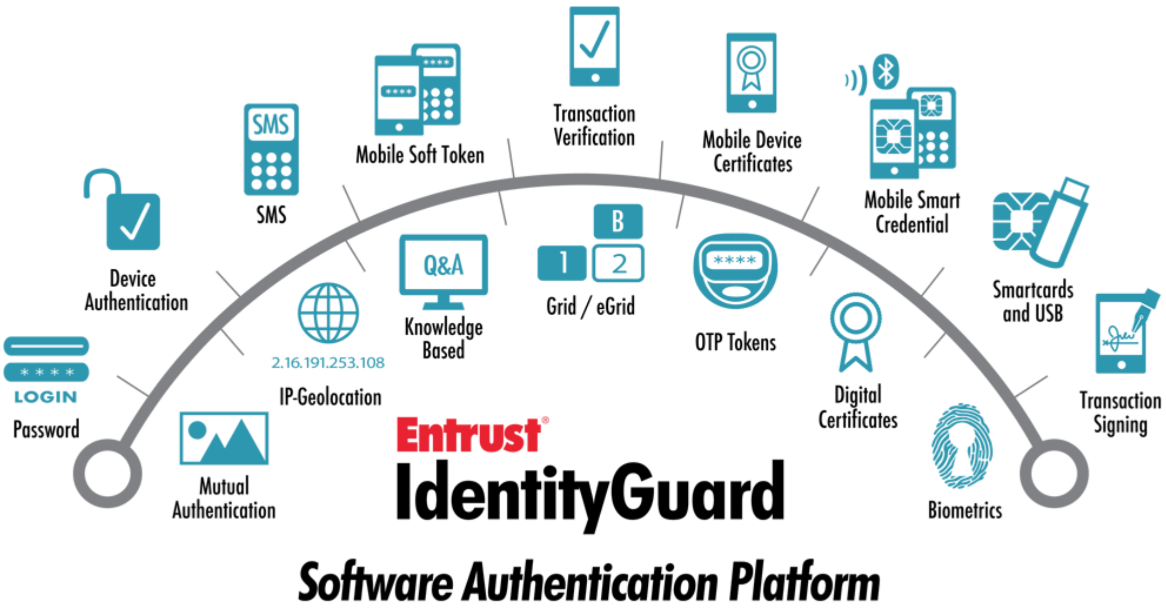
If Entrust IdentityGuard itself is set up at the customer's facility for PIV-I issuance, then cards must be issued after the installation and then tested by a government-sponsored lab to ensure compliance. This is included in the Entrust service.

The Entrust Difference: One Platform, All Approved Authenticators

The Entrust solution for strong authentication for healthcare organizations provides all approved authenticators from a single platform.

The organization may deploy different authenticators to different employees to minimize the investment in both the cost of the credential and the time required by the employee to complete the identity-proofing.

Rather than purchasing a one-time-password solution to achieve assurance for Overall Level 2, and another solution for FBCA Medium hardware smartcards for assurance to Overall Level 4, organizations may purchase and deploy, operate and manage just one platform.



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