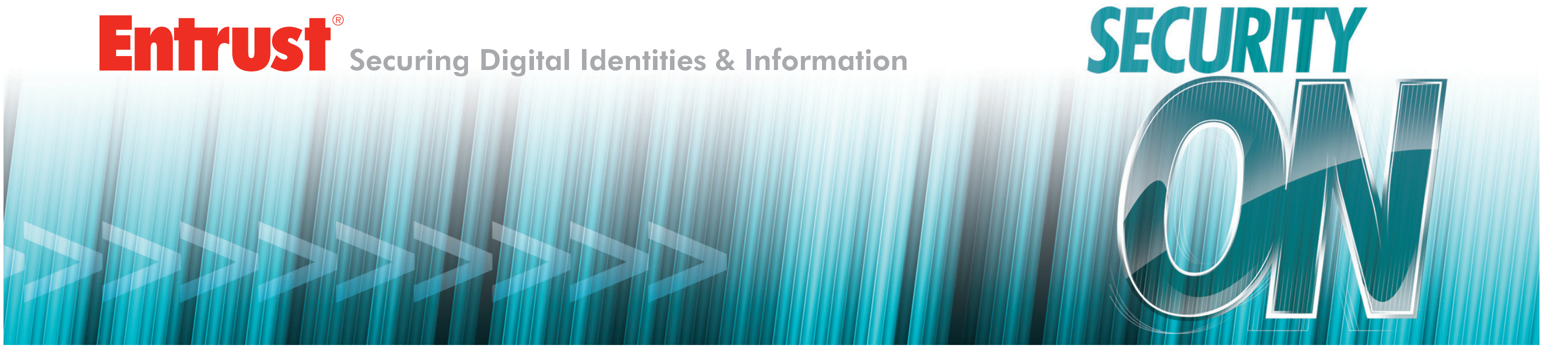
Entrust® Securing Digital Identities & Information



Turnkey Authentication for Government Contractors

Federal Bridge CA & HSPD-12 Solutions

The protection of government assets starts with a secure, trusted identity. Many U.S. government agencies mandate that usernames and passwords are no longer an acceptable form of authentication to government Web portals.

As part of the Non-Federal Identity Shared Service Provider (NFI-SSP) public key infrastructure (PKI) program, the U.S. government requires the use of smartcards with digital certificates issued by an approved certification authority (CA) that's cross-certified with the U.S. Federal Bridge CA (FBCA).

Entrust's Non-Federal Identity Shared Service Provider PKI & Smart Credential solution enables government agencies to issue and distribute identity credentials to third-party contractors for authenticated access to sensitive information, applications and databases.

Authenticating Non-Federal Identities

While the U.S. government has long had strong and reliable methods for authenticating government employees, they also require a similar solution to securely verify the identities of non-federal, third-party contractors, consultants and staff. Multipurpose smartcards have proven secure and effective.

With smartcards, digital identities are much more difficult to compromise when compared to other methods, such as usernames and passwords or one-time-passcode (OTP) tokens. The digital identity never leaves the card; rather, the Web portal sends a request to the card to prove it has the digital identity. A PIN is required, so the card will only authenticate the rightful owner.

Federal Bridge CA policies require that a person undergo diligent identity-proofing before being issued a digital identity. This provides contractors with a secure trusted identity to access government Web portals.

Solution Benefits

- Issue and distribute credentials to third-party contractors for authenticated access to sensitive information, applications and databases
- Enable cross-certification with the U.S. Federal Bridge Certification Authority (FBCA)
- Streamline vetting and management of digital identities
- Comply with HSPD-12, FIPS 140 and 201 requirements for interoperability
- Reduce costs and need for on-staff expertise with Entrust's cloud-based services, which offer hosted smart credentials and PKI
- Leverage credential investment for authenticated access to approved cloud applications and services
- Complement PKI solutions with advanced capabilities from the Entrust IdentityGuard software authentication platform

Industry Trust
Federal Bridge CA policies require organizations in various verticals to use trusted identities to access government Web portals.

- Healthcare Organizations
- Private & State Universities
- Law Enforcement Groups
- Transportation Workers
- Public & Private Enterprises
- U.S. Department of Defense Contractors

GOVERNMENT-GRADE SECURITY

Entrust provides secure, trusted identities that empower government agencies or enterprises with the choices necessary to enable business. Whether issued from Entrust's cloud-based services or via an in-house deployment model, Entrust provides an end-to-end solution for issuing, distributing, managing and revoking digital identities across large user populations. Both hosted and on-premise offerings provide organizations a Non-Federal Identity SSP PKI solution.

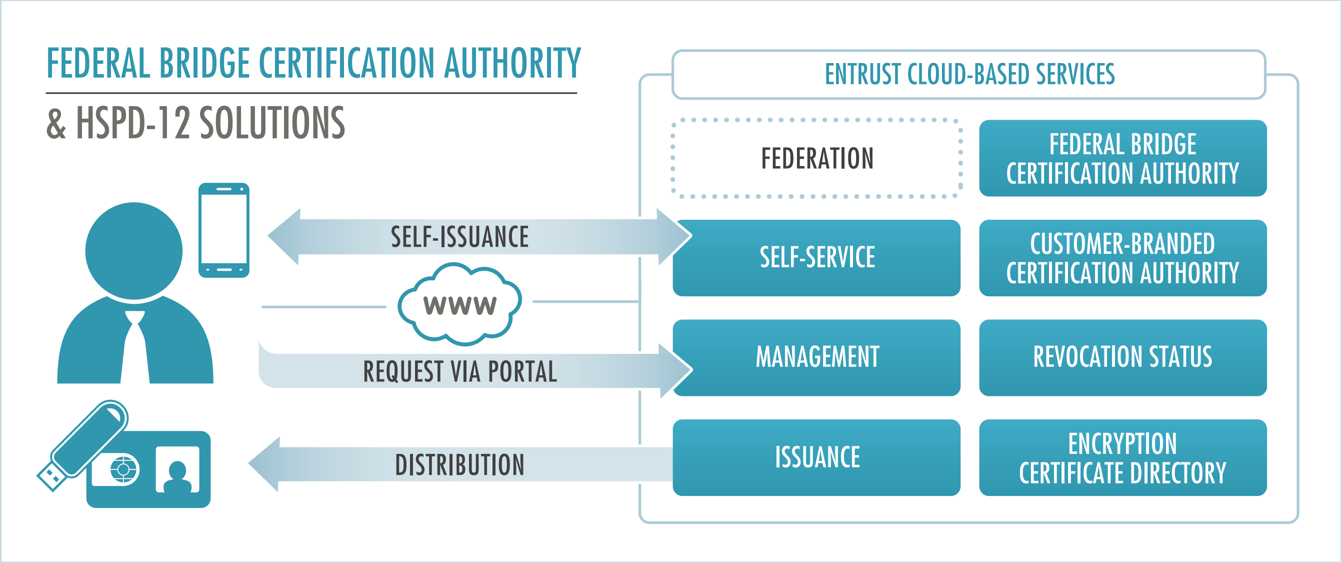

FEDERAL BRIDGE CERTIFICATION AUTHORITY
& HSPD-12 SOLUTIONS
ENTRUST CLOUD-BASED SERVICES
FEDERATION
FEDERAL BRIDGE CERTIFICATION AUTHORITY
SELF-ISSUANCE
SELF-SERVICE
CUSTOMER-BRANDED CERTIFICATION AUTHORITY
WWW
REQUEST VIA PORTAL
MANAGEMENT
REVOCATION STATUS
DISTRIBUTION
ISSUANCE
ENCRYPTION CERTIFICATE DIRECTORY

Figure 1: Entrust's end-to-end solution enables U.S. government agencies to issue, proof, manage or revoke digital identities assigned to authorized third-party contractors.

Global Smartcard Issuance & Management

Entrust's comprehensive platform approach enables governments to issue and manage smartcard populations — whether locally or across the globe. This seamless method makes it efficient to displace outgoing legacy systems or simply issue a credential for a new employee — all from a comprehensive platform.

Proven Hosted Model

Harness the power of PKI technology without buying, establishing or operating an in-house CA. The Entrust Non-Federal Identity SSP PKI provides U.S. government customers a proven, easy-to-use method for issuing cross-certified identity credentials to third-party contractors — and it's all securely managed in the cloud by Entrust's PKI experts.

For organizations seeking a complete solution that includes both smartcards and the underlying PKI, Entrust's cloud-based offering provides smart credentials and a built-in Non-Federal Identity SSP PKI.

The solution simplifies the entire process of provisioning, managing and deploying smart credentials. And all technology is pre-packed and provisioned straight from the cloud.

Identity-Proofing

Entrust's solution offers trusted identity-proofing to U.S. federal government standards, which allows for three assurance levels:

- **Rudimentary** — Verify the credential owner has, in their possession, the email address defined in the certificate.
- **Basic** — Verify the credential owner is in possession of a physical address.
- **Medium** — Verify the credential owner's identity through a face-to-face meeting to check government-issued identity documents, or through a series of online questions that only the true owner knows.

For CAs operating outside the federal jurisdiction, Entrust provides a choice of tools that may be leveraged to automatically prove credential owner identities.

Secure Production

Entrust smartcards are printed with digital identities in a secure facility, delivered and distributed following simple guidelines for identity-proofing.

Flexible Form Factors

Each government contractor is given the option of a FIPS 140-certified smartcard or, for those who do not possess a card reader, a USB form factor.

These chip-based smart credentials contain microprocessors that compute, in real time, cryptographic operations that validate and authenticate users. And since they are effectively embedded computers, they are able to store a variety of identity information (e.g., fingerprint or retina scan).

For HSPD-12, the FIPS 201-certified smart credential delivers guaranteed interoperability with Microsoft Windows 7 and a wide range of third-party products. To ensure compatibility, Entrust can provide drivers for legacy Microsoft Windows XP environments.

ENTRUST IDENTITYGUARD

Benefit from the award-winning, on-premise Entrust IdentityGuard software authentication platform, which provides advanced technology for strong authentication and identity management. Deploy strong authentication throughout a government department or agency, enable physical, logical and cloud access control, and secure or leverage authorized mobile devices and identities co-existing within a given environment.

Mobile Identities

Available on today's most popular mobile platforms, including Apple iOS, Google Android™ and BlackBerry®, Entrust mobile security solutions help organizations issue digital identities to smartphones. This is convenient for employees or contractors who do not require access to government portals, but use the same digital identities for authentication, digital signing and encryption.

Federation Capabilities

The Entrust IdentityGuard Federation Module helps organizations leverage smartcards for authenticated access to SAML-capable applications and services, including third-party resources like Microsoft 365 and Salesforce.com, which reduces reliance on usernames and passwords.

API Integration

Entrust's open API architecture allows for tight integration with today's leading mobile device management (MDM), identity access management (IAM) and public key infrastructure (PKI) vendors. This enables Entrust IdentityGuard to work with new and existing enterprise implementations, plus adds the ability to integrate in-house or managed service-based digital certificates.

All Authenticators, One Platform

Entrust offers the full range of authenticators issued from a common workflow and managed by a common administration capability, helping simplify compliance audits.

Entrust's diverse set of authentication capabilities include smartcards and USB tokens, soft tokens, grid cards and eGrids, IP-geolocation, questions and answers, mobile smart credentials, out-of-band one-time passcode (delivered via voice, SMS or email), out-of-band transaction verification and a range of OTP tokens.

Mobile Smart Credentials

Mobile smart credentials are virtual smartcards embedded onto a mobile device and are available on a variety of market-leading mobile platforms, such as Apple iOS, Android and BlackBerry. Dramatically reduce costs by using either employed-purchased (i.e., Bring Your Own Device) or corporate-issued devices instead of purchasing tokens or physical smartcards.

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 affordable in today's uncertain economic climate.

The smart choice for properly securing digital identities and information, Entrust solutions represent the right balance between affordability, expertise and service.

For more information on Federal Bridge CA & HSPD-12 Solutions, contact the Entrust representative in your area at **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, TX 75240 USA

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

About Entrust
A trusted provider of identity-based security solutions, Entrust secures 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 **www.entrust.com**.

Entrust® Securing Digital Identities & Information