Entrust Derived PIV Credential Solution

A guide to meet NIST SP 800-157 requirements

ENTRUST

SECURING A WORLD IN MOTION

Table of Contents

Introduction: The need for mobile credentials 3

Entrust: The most complete derived PIV credential solution................... 4

Use cases: Getting the most out of your mobile smart credential........12

Conclusion 15

INTRODUCTION

The need for mobile credentials

In an ever-reaching digital world, mobile is transforming organizations by providing employees with the freedom and ease of anytime, anywhere access to applications, resources, and information. As the mobile workforce continues to grow, and employees leverage mobile as their primary computing platform, this new frictionless environment will help to optimize productivity, serve customers better, and reduce overhead. From inspectors to social services workers to business owners, mobile devices allow employees instant access to the information they need to be more effective in performing their jobs.

As organizations shift to mobile, ensuring the authenticity of the individuals accessing sensitive information and protecting that information in the field becomes even more important. In order to do this, a trusted digital identity is key for users accessing resources and conducting transactions. Unfortunately, traditional approaches to identity and access management do not translate well into the mobile world. Usernames and passwords can be programmed into mobile devices for quick access, but they are insecure, inconvenient to reset, and cause friction for the user. Stronger authentication methods – including one-time password (OTP) tokens – hinder the mobile user experience, and traditional methods such as smart cards simply can’t be easily and cost-effectively inserted into tablets and phones.

The U.S. government has made a large investment in the HSPD-12/FIPS 201-2 Personal Identity Verification (PIV) program to ensure the integrity of data and the individuals accessing data. However, because this program is smart-card-based, it is difficult to transfer to a mobile platform, where smart cards cannot be effectively used without significant user impact. Recognizing the benefits of a mobile platform, the National Institute of Standards and Technology (NIST) developed Special Publication 800-157 - to provide a guide as to how the PIV credential can be used to create a new and trusted credential directly on mobile devices. This allows organizations to leverage mobile devices while remaining compliant with the HSPD-12/FIPS 201-2 Personal Identity Verification (PIV) requirements.

Entrust: The most complete derived PIV credential solution

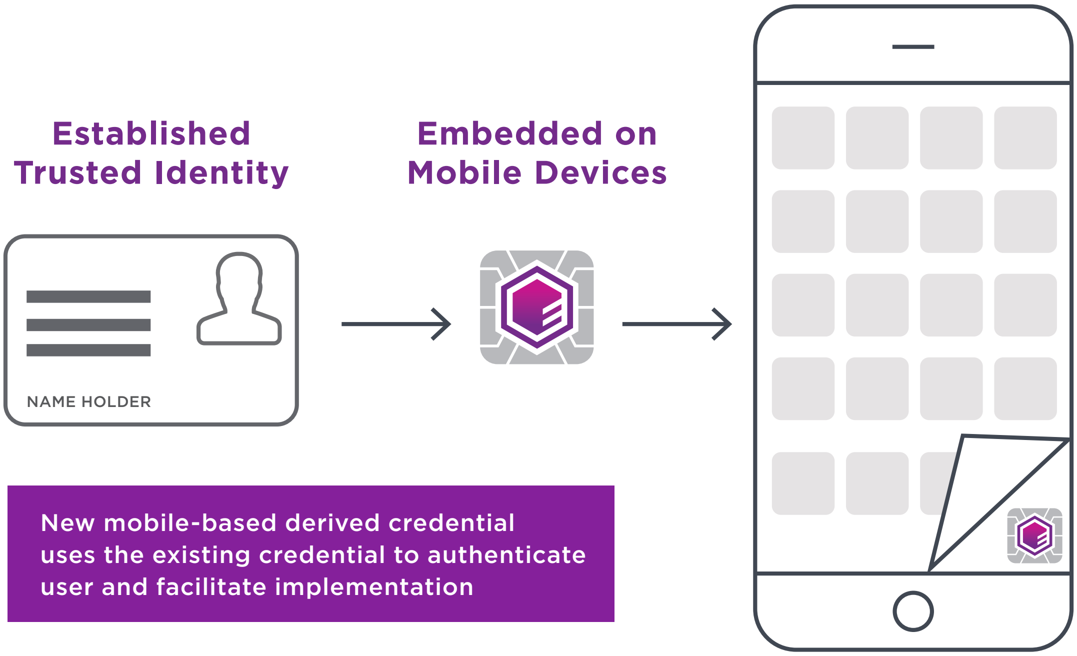
Entrust's solution addresses the key elements required to properly enable a seamless and secure transition to a mobile platform.

Derived PIV credentials defined

The Entrust Derived PIV Credential solution provides government agencies and contractors with a comprehensive, frictionless, and proven solution by placing a PIV smart credential onto mobile devices, enabling mobile as the computing platform.

The enrollment process leverages the user's existing PIV smart card to authenticate them before "deriving" or creating a new, unique mobile credential that is installed onto their mobile device: a derived PIV credential. By leveraging the user's existing PIV, Entrust simplifies the enrollment and management process, maintaining the integrity of the system while extending the capabilities of HSPD-12 credentials.

While the authentication of the user prior to the issuance of the derived PIV credential comes from the user's existing PIV smart card, the resulting derived PIV credential is unique and independent from the user's PIV smart-card-based credential. This process is similar to using government-issued credentials such as your driver's license and passport to verify your identity when getting a PIV card. Once the PIV card is issued, the user has a trusted credential that is separate from their driver's license and passport, and can be managed independently. Similarly, once the derived PIV credential is issued, the user has two unique and valid credentials associated with their account that can be managed independently. One is on a smart card, the other is on their mobile device.



New mobile-based derived credential uses the existing credential to authenticate user and facilitate implementation

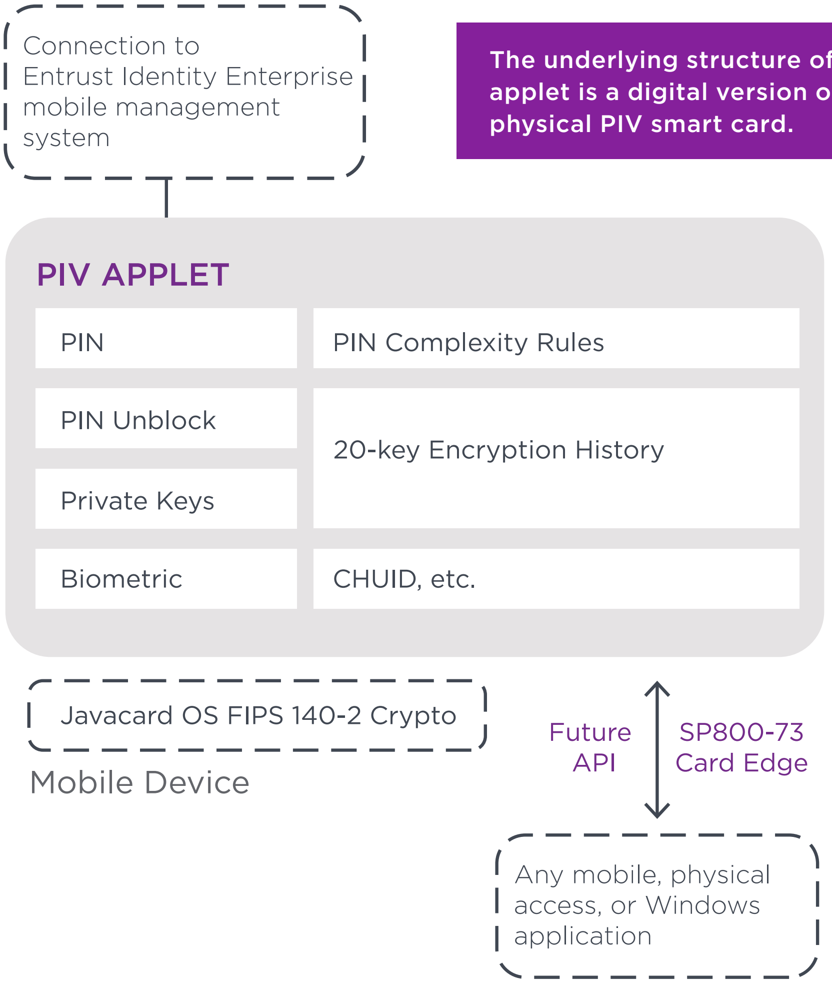
Entrust Derived PIV Smart Credential solution

Following the specifications defined in NIST SP 800-157, Entrust developed its Entrust Identity mobile application as a full-featured, enterprise-ready solution for derived PIV credentials that meets U.S. federal government specifications.

The Entrust Identity mobile application, downloaded to the user's device, is encoded like a PIV smart card, with a digital structure that follows the current PIV standard. This allows the application to be encoded by Entrust Identity Enterprise with certificates that use the same communication language used on a physical PIV smart card. It results in seamless interoperability with existing PIV-enabled websites and applications. The PIV-enabled application views the derived PIV credential in the same way it would interact with a traditional PIV smart card.

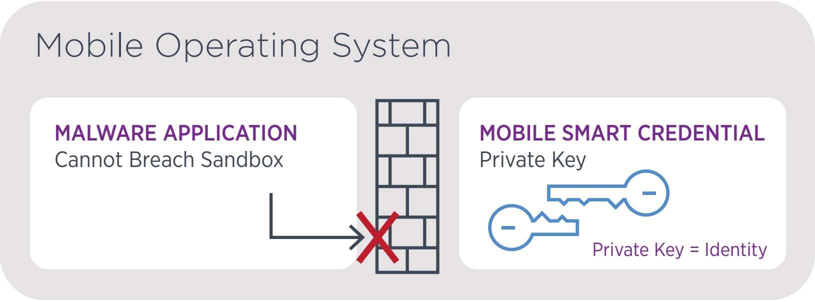
The Entrust Identity mobile application is available for use on Apple iOS and Google Android mobile operating systems.

The underlying structure of the Entrust Identity PIV applet is a digital version of the chip found on a physical PIV smart card.


Connection to Entrust Identity Enterprise mobile management system
PIV APPLET
PIN
PIN Complexity Rules
PIN Unblock
20-key Encryption History
Private Keys
Biometric
CHUID, etc.
Javacard OS FIPS 140-2 Crypto
Mobile Device
Future API
SP800-73 Card Edge
Any mobile, physical access, or Windows application

Leveraging the mobile architecture for added security

The mobile device architecture inherently adds security over the desktop architecture. Applications on a mobile device are independent of other mobile applications. Each mobile application exists in a virtual sandbox, separated from the other applications installed on the same device. The benefit of this architecture is that it is resistant to malware prevalent in traditional desktop computers. Because each application is independent of the other applications, an exploit of one application does not threaten other applications on the phone. An exploit cannot 'jump applications' but is restricted to the affected application. This is contrary to the shared memory space of a traditional desktop computer where a compromise of one part of the computer gives the attacker easy access to other parts of the computer.



Security is strengthened by a virtual "sandbox" created by the mobile operating system. This provides enhanced security over traditional desktop-based applications.

Digital certificate storage and access

Native keystores

Mobile devices have a built in 'native' keystore where digital certificates for authentication, encryption, and/or signing can be housed.

Native keystores provide operating system (OS) layer protection of the keys. iOS and Android devices restrict access to the digital certificates stored in the native keystore to applications ONLY developed by the OS manufacturer (such as email, calendar, contacts, and the web browser applications). A select group of third-party vendors, including a number of mobile device management (MDM) vendors have also negotiated access to the native keystores. These vendors have a defined set of applications that are integrated with the native keystore. For derived PIV credentials, Entrust ensures that enrollment of the derived PIV credential into the native keystore is performed in a manner that is compliant with NIST SP 800-157 policy. Additionally, compatibility with the derived PIV credential issuance software must be maintained with each new version of the mobile device manufacturer OS issued by the mobile device vendor (typically released each year).

Leveraging the mobile vendor keystore for certificate storage and use may be acceptable for organizations that only require the use of the limited number of applications that the mobile device manufacturer provides (email, web browser, contacts, and calendar) or the select third-party vendors who have integrated with the native keystore.

Entrust keystore

All applications that do not have access to the native keystore, including any custom, mission-specific applications, must use a different keystore to house digital certificates used by the applications for authentication, encryption, and/or signing purposes.

Entrust has leveraged its history as the world's leading PKI company and long-term partner to the U.S. federal government to ensure that keys stored and managed by the Entrust Derived PIV Credential solution meet U.S. federal government standards.

Keys stored in the Entrust keystore have OS layer protection of the keys. However, to ensure the integrity of the keys, Entrust has added additional protection measures. Leveraging the security provided by mobile device operating systems, the Entrust Identity mobile application is encrypted using strong cryptographic processes tied to unique characteristics of the specific mobile device where the application is installed. This helps ensure that the private keys are accessible only on the same device where the keys were initially created. This prevents the keys from being copied and used on an unauthorized device or application, in the unlikely event that the sandbox is breached. In addition, access to the Entrust Derived PIV Credential is PIN-protected, providing a defense against brute force attacks as well as access to the credential if a device is lost or stolen.

Entrust's solution design allows it to partner with the leading MDM and independent third-party application vendors to ensure the proper integration with their applications and the Entrust Derived PIV Credential solution. These close relationships ensure both companies can support customers' existing and new requirements in a timely fashion, without requiring customers to perform and maintain the costly integration work surrounding both third-party and native applications. This provides a more transparent and streamlined solution.

Leveraging the Entrust keystore for certificate storage may be more appropriate for organizations that want higher certificate protection or who need the flexibility to leverage third-party or custom applications to meet organizational objectives.

NIST SP 800-157 allows for two different levels of assurance for the derived PIV credential. These levels are referred to LOA-3 and LOA-4. LOA-4 and require special hardware to be attached to the mobile device. Due to mobile OS technology limitations, only third-party keystores on iOS and Android are currently supported for LOA-4 solutions. While the Entrust Derived PIV Credential solution can support LOA-4 enrollment, only the LOA-3 workflows will be presented in this document.

Issuance and enrollment

Entrust has formed relationships with the leading MDM vendors who support mobile-first governments and enterprises. These partnerships allow organizations to leverage their existing MDM investment for the deployment and ongoing management of the mobile devices and applications. For organizations who do not currently use an MDM solution, the Entrust Identity mobile application solution can be effectively deployed and managed through our award-winning Entrust Identity Enterprise platform.

NIST SP 800-157 allows a user to complete the issuance and enrollment of a derived credential by leveraging the strong identity binding associated with their current valid PIV smart card. By leveraging the Entrust self-service portal, PIV and CAC smart card users can request a derived PIV credential using their PIV or CAC smart card for identity verification instead of going through a face-to-face identity verification process.

The Entrust browser-based self-service portal eliminates the need for client-side software, creating a frustration-free administrative experience. This clientless deployment, coupled with the industry-leading user self-directed enrollment, limits administrative overhead, and leads to significant cost savings compared to other vendor solutions.

Derived PIV credential enrollment for third-party COTS applications:

An employee receives their mobile device, and has already gone through the organization's approval for a derived PIV credential.

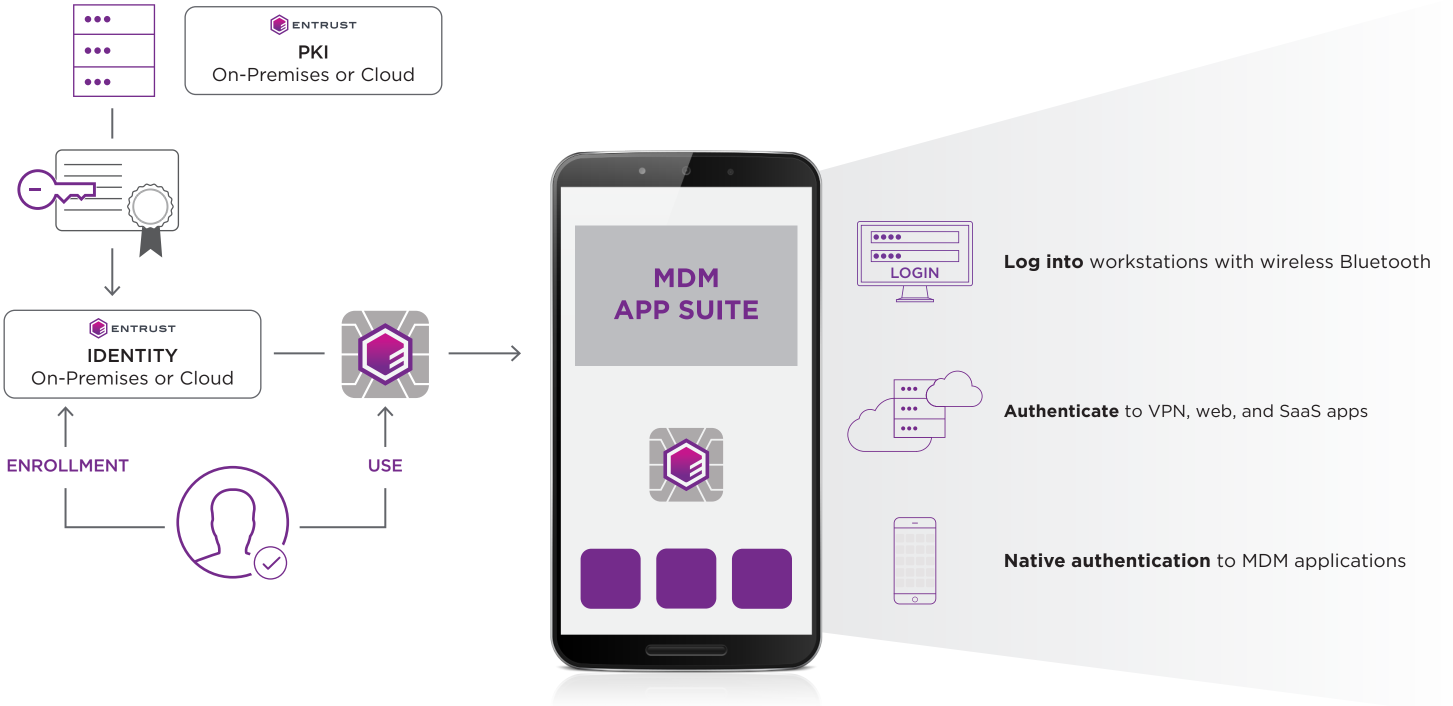
At this point, the employee is sent a link to the Identity Enterprise Self-Service Module web portal. From their physical workstation, the employee logs into the web portal with their PIV/CAC Authentication certificate. The employee's PIV/CAC authentication certificate is validated, and checked to ensure it was issued from an approved certification authority, and has the correct PIV/CAC authentication OID for strict NIST SP 800-157 compliance. Additionally, a copy of this PIV/CAC authentication certificate is stored, along with the time of authentication, to allow the certificate to be checked for revocation seven days after derived PIV credential issuance.

Once the employee has authenticated, they select the link to request a derived PIV credential from within the web portal. After clicking the link, the Identity Enterprise Self-Service Module uses the PIV authentication certificate to build the contents of the derived PIV credential certificate to be issued to the user. This eliminates the need for an administrator to manually enter the contents for each employee's derived PIV credential certificate.

The web portal then provides an encrypted activation link to the employee, to be opened on the employee's mobile device. This activation link can be provided either by email, or within the secure TLS browser session in the form of a QR code. To decrypt the activation link, the employee is given a FIPS compliant one-time password (OTP). This OTP can be delivered to the user either by an encrypted email, which is encrypted by the user's encryption key issued to their physical PIV smart card, or can be presented visually within the secure TLS browser session. For email delivery options of both the encrypted activation link and OTP, the email address is the same as the RFC822 email field associated with the employee's PIV authentication certificate used to request the derived PIV credential. All of the necessary information required to build and bind the derived PIV credential is pulled by the Self-Service Module, and can be configured to require no administrative involvement.

The employee then opens the activation link on their mobile device.

After opening the activation link, the employee selects the option to begin the activation process from within the secure derived PIV credential keystore application. At this time, the derived PIV authentication key, as well as any additional digital signature keys, are generated within the secure crypto module of the mobile device. If encryption keys are to be included with the derived PIV Credential, these keys are securely recovered from the PIV issuing CA (if policy allows), and are securely delivered to the secure third-party derived PIV credential keystore application. The derived PIV credential enrollment method is completed.


ENTRUST
PKI
On-Premises or Cloud
ENTRUST
IDENTITY
On-Premises or Cloud
ENROLLMENT
USE
MDM
APP SUITE
LOGIN
Log into workstations with wireless Bluetooth
Authenticate to VPN, web, and SaaS apps
Native authentication to MDM applications

The Entrust Identity mobile application, downloaded to the user's device, is encoded like a PIV smart card, with a digital structure that follows the current PIV standard.

Derived PIV credential enrollment for native OS applications for iOS and Android:

An employee receives their mobile device, and has already gone through the department's approval for a derived PIV credential. At this point, the employee is sent a link to the Identity Enterprise Self-Service Module web portal. From their physical workstation, the employee logs into the web portal with their PIV authentication certificate. The employee's PIV authentication certificate is validated, and checked to ensure it was issued from an approved certification authority, and has the correct PIV authentication OID for strict NIST SP 800-157 compliance. Additionally, a copy of this PIV authentication certificate is stored, along with the time of authentication, to allow the certificate to be checked for revocation seven days after derived PIV credential issuance.

Once the employee has authenticated, they select the link to request a FIPS compliant OTP. This OTP is delivered to the employee's government email. Using their mobile device, the employee navigates to the Identity Enterprise Self-Service Module web portal using their native mobile browser application, and logs in using the OTP delivered to their government email. From their authenticated session on their mobile device, the employee selects the link to request a derived PIV credential for the native keystore. This begins the activation process.

If the employee's mobile device is an iOS platform, the derived PIV authentication key, as well as any additional digital signature keys, are generated within the native keystore of the iOS device using the SCEP protocol. If the employee's mobile device is an Android platform, the derived PIV authentication key, as well as any additional digital signature keys are packaged into a p12 file, and delivered to the mobile device through the secure TLS browser session. For either platform, if encryption keys are to be included with the derived PIV credential, these keys are securely recovered from the PIV issuing CA (if policy allows), and are securely delivered to the platform's native keystore application using SCEP for iOS and p12 delivery for Android.

Ongoing management self-service capabilities

In comparison to other derived credential solutions, Entrust Identity Enterprise is unique in its ability to allow users to request and manage their derived PIV credentials through the Entrust Self-Service Module (SSM) without the need for administrative interaction.

The Entrust Identity Enterprise SSM can be deployed in a high-availability architecture, with only a few servers deployed locally to service users around the world. This approach greatly increases scalability and reliability, and reduces operational costs by limiting the need to deploy specialized enrollment stations and kiosks abroad for derived PIV credential enrollment. Users are able to access the SSM from any workstation with a working smart card reader and request or manage their derived PIV credentials.

The Entrust Identity Enterprise SSM is accessed through a web-based interface that is configured to require the PIV authentication certificate to log into the User Self-Service Module. Additionally, the Entrust Identity Enterprise system can require the user's PIV credential to contain a registered PIV authentication OID. This secures the Entrust Self-Service Module to only allow authorized users to log in with valid, U.S. federally issued PIV authentication credentials for strict NIST SP 800-157 adherence. This ensures the derived PIV credential will have the proper identity binding to the user's PIV smart card, and securely protects against unauthorized users logging into the Identity Enterprise system.

The broad range of services provided by government agencies and the organizations that support them often requires employees to be away from their departments and their IT support services. Having a secondary mobile-based HSPD-12 credential that is easily and securely self-managed reduces the likelihood of a remote employee being unable to log into their workstation or access services due to damage to their credential or being locked out because of a forgotten PIN.

Unlike PIV smart cards, PIN unblock and reset is easily self-managed through both the Entrust Identity Enterprise SSM and directly on the mobile device through the Entrust Identity mobile application. If the user loses their mobile device or feels their credential has been compromised, the SSM allows for the derived credential to be quickly suspended or revoked. The user can then enroll for a new derived PIV credential on their new or existing mobile device.

Policy adherence and compliance

The Entrust solution's issuance and enrollment process also addresses a number of the key policy issues pertaining to derived PIV credentials.

PIV authentication and certificate validation

- Depending upon the assurance level, derived PIV credential solution issuance systems must recheck the PIV/CAC authentication certificate seven days after issuance
  - The Entrust Derived PIV Credential solution includes this capability out of the box

PIV eligibility revocation and derived PIV revocation

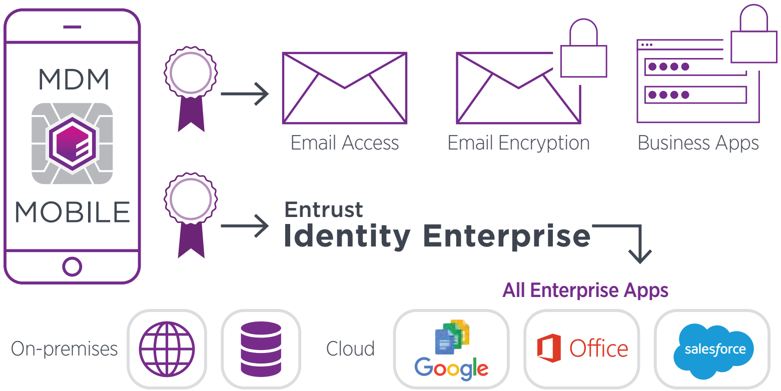
- Once a user is no longer eligible to hold a physical PIV card, their derived PIV credential be revoked
  - The Entrust PIV Credential Solution has fully available APIs for synchronizing the derived PIV credential revocation against PIV eligibility, ensuring the solution is fully consistent with the standard without the need for expensive, one-off customizations

Issuing CA must be an authorized FED SSP for PKI

- Only the existing U.S. federal PIV providers are authorized to issue derived PIV credentials
  - Entrust is the only vendor that can provide a complete end-to-end derived PIV credential solution

Use cases: Getting the most out of your mobile smart credential

Once deployed, the Entrust Mobile Derived PIV Credential allows mobile workers the ability to leverage their mobile devices to securely access information and complete transactions anytime, anywhere.



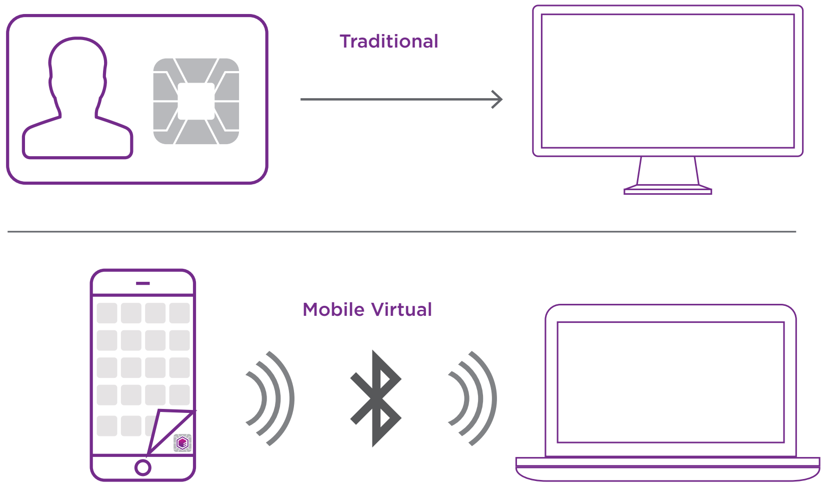
Accessing web applications

Having secure access to data whenever and wherever you need it greatly improves productivity and accuracy. Protecting access to the information in the field through insecure networks is critical to protect the rights of individuals, and to provide public confidence in the system. Entrust addresses this issue in a number of ways to give organizations implementation flexibility. Through Entrust's integration with MDM vendors and independent third-party web browsers, we provide safe, PIV-certificate-based access to web applications. For web applications and web portals that support PIV-based authentication today, this capability is enabled with no change to the existing infrastructure. Whether the user is accessing the OS native browser, MDM integrated browser, or a specialized third-party browser, the Entrust derived credential solution can issue and manage a derived PIV credential to meet the needs of an organization.

Digitally sign documents

A large remote and distributed workforce is increasing the need for digital signature capabilities. Because of Entrust Derived PIV Credential's ability to store and use signing certificates, through integration with digital signing applications, employees can digitally sign requests anywhere. This means food inspectors can complete, sign, and submit their reports in the field, contracts can be signed and filed from the employee's home, and police officers can request and receive a signed warrant without ever leaving a potential crime scene.

Automatically log onto and off of desktops



Entrust's derived credential provides a solution for both traditional smart card logon using a mobile smart credential, as well as accessing PIV-enabled applications directly through a mobile device.

Government employees are comfortable using their PIV smart cards for logical access to their workstation or laptop. While this is an effective method of user authentication, it also presents challenges. Most organizations have a policy that desktops must be locked when the user is away. To do so, the user must remove their smart card from the smart card reader to log off. Oftentimes the user will forget or intentionally leave their smart card inserted when leaving their workstation, which presents a serious security vulnerability and puts the employee and constituent data at risk.

The Entrust Identity mobile application can be paired with workstations through Bluetooth or NFC (depending on the device). This allows the workstation to 'recognize' the user's derived PIV credential as they approach the workstation, and asks them to authenticate with the derived PIV credential. Once the user is authenticated and the Entrust Identity mobile application is connected to a workstation, the mobile device operates much in the same way as a traditional physical smart card.

The Entrust Identity mobile application continues to operate like a physical PIV smart card, with the public certificates being made available to other applications through Microsoft Cryptographic Application Programming Interface (CAPI). This allows seamless integration with existing PIV-enabled applications such as the Microsoft Office suite, including Outlook. The mobile-based derived credential provides almost the same smart card logon experience that a user expects when using their PIV smart card, reducing the amount of training required to use the derived Entrust Identity mobile applicationl.

If desired, Entrust's derived PIV credential can be enabled to automatically lock the Microsoft Windows operating system when the mobile device is taken out of a configurable Bluetooth range from the user's workstation. Users are less likely to leave their mobile device at their desk when they go to lunch or take a break, resulting in fewer instances of unattended workstations remaining logged in to sensitive networks.

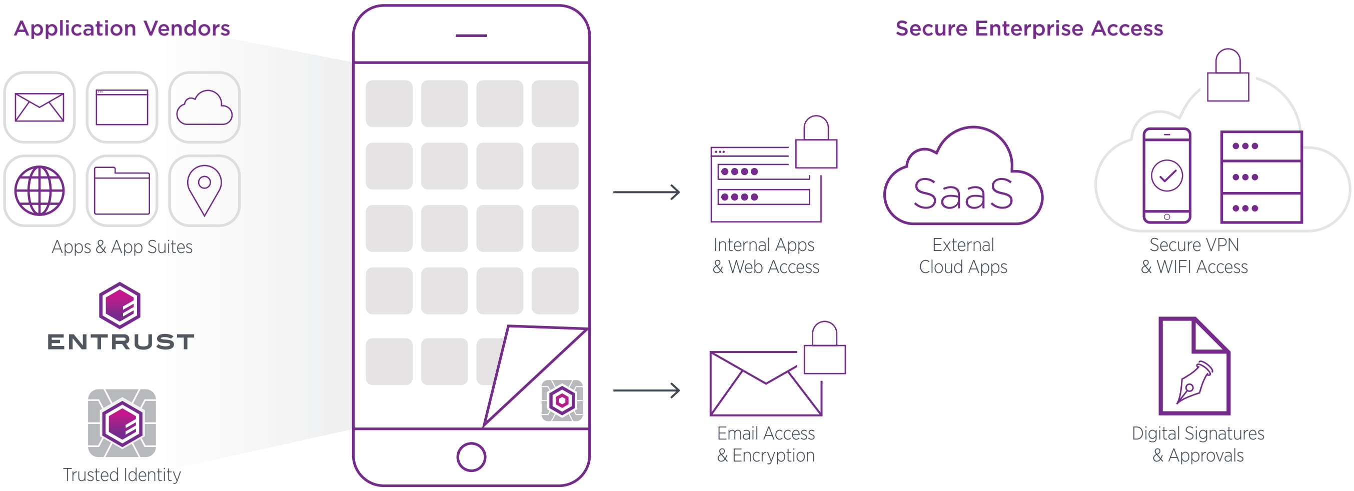
Strong certificate-based security to third-party applications

In order to reach the full potential of the Entrust derived PIV credential, it is important that it can integrate into an organization's existing application ecosystem.

Entrust has technology partnerships with key MDM vendors including Microsoft, IBM, MobileIron, and VMware. These integrations allow the MDM vendor applications to use the derived PIV credential for strong PIV-certificate-based user and device authentication prior to accessing resources.

Other third-party integrations exist today to meet key organizational requirements. Examples include Thursby, Juniper Junos, Acronis, and Monkton's derived PIV credential solution.

Entrust's broad suite of integrations enable organizations to leverage the application environments that best suit their needs while providing a secure and consistent approach to NIST SP 800-157 compliance. In addition, the Entrust Derived PIV Credential solution has open APIs and a SDK format that lends itself to easy and direct integration with the solution. These various integration points and our support of both on-premises and managed service deployment options ensure that the Entrust solution can meet the demands of any organization's mobile needs.



Entrust's Derived PIV Credential offers simple integration with many leading applications – either directly through the mobile device or via smart card logon from a traditional workstation.

Conclusion

Organizations and their employees want a frictionless experience that allows them to be productive and ultimately provide better customer service. Mobile computing provides the opportunity for employees to use the device they love most, gain secure access to information in the field, and to complete transactions.

The HSPD-12/FIPS 201-2 Personal Identity Verification (PIV) program and NIST SP 800-157 provide the framework to do this in a secure manner that protects both the employee and the customers they serve. Entrust solutions, in conjunction with key partners, provide agencies and supporting organizations the ability to implement a program that meets user needs while remaining compliant with federal regulations.

For more information

888.690.2424
+1 952 933 1223
info@entrust.com

entrust.com

ABOUT ENTRUST CORPORATION

Entrust secures a rapidly changing world by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com