ENTRUST DATACARD DERIVED PIV CREDENTIAL SOLUTION

A Guide to Meet NIST SP 800-157 Requirements

Table of contents

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 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 inserted onto tablets and phones.

The US Government has made a large investment in the HSPD12 / FIPS 201 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, NIST developed **Special Publication 800-157** - which provides 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 HSPD12 / FIPS201 Personal Identity Verification (PIV) requirements.

Entrust Datacard: The Most Complete Derived PIV Credential Solution

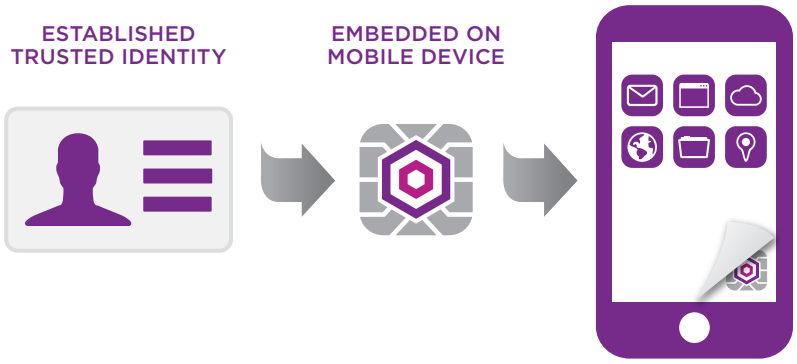
Entrust Datacard's solution addresses the key elements required to properly enable a seamless and secure transition to a mobile platform.

Derived PIV Credentials Defined
The Entrust Datacard 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 users existing PIV Smart Card to authenticate the user before 'Deriving' or creating a new, unique mobile credential that is installed onto the users mobile device: a Derived PIV Credential. By leveraging the users existing PIV credential to validate the user, Entrust Datacard 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 users 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 the 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 which 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

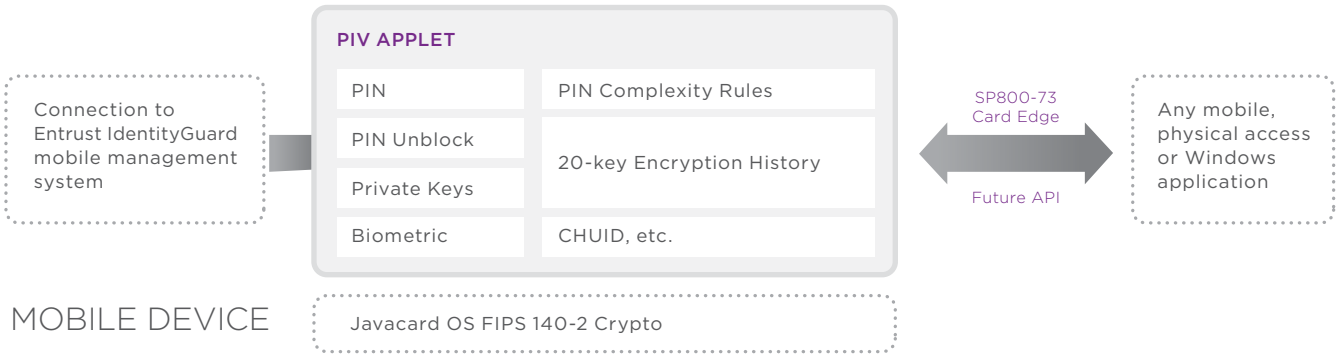


Entrust Datacard Derived PIV Smart Credential Solution
Following the specifications defined in NIST SP 800-157, Entrust Datacard developed its Mobile Smart Credential Application (MSC) as a full-featured, enterprise-ready solution for derived PIV credential that meets US Federal Government specifications for Derived PIV Credentials.

The Entrust IdentityGuard Mobile Smart Credential application, downloaded to the user's device, is encoded like a PIV smartcard, with a digital structure that follows the current PIV standard. This allows the Mobile Smart Credential to be encoded by Entrust IdentityGuard with certificates that use the same communication language used on a physical PIV smartcard. This 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 smartcard.

The Entrust IdentityGuard Mobile Smart Credential is available for use on Apple iOS, Google Android and BlackBerry mobile operating systems.

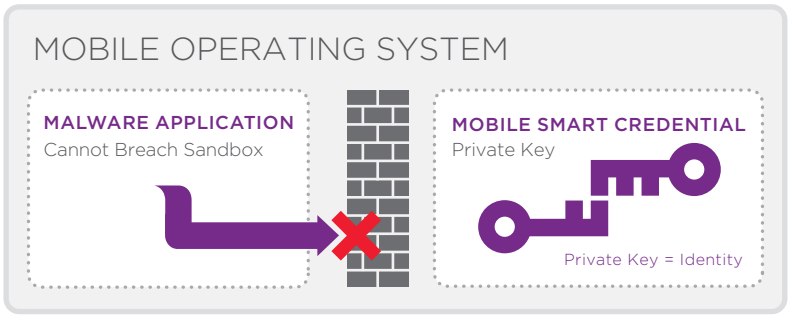
The underlying structure of the Entrust Mobile Smart Credential PIV applet is a digital version of the chip found on a physical PIV smartcard.



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 applications does not threaten other applications on the phone as 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 Enterprise Mobility Management (EMM) vendors have also negotiated access to the native keystores. These vendors have a defined set of applications that are integrated with the native key store. 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 Datacard's PKI expertise and partner ecosystem ensure success and security."

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 Datacard has leveraged its history as the world's leading PKI company and long term partner to the US Federal Government to ensure that keys stored and managed by the Entrust Datacard Derived PIV Credential solution meet US Federal Government standards.

Keys stored in the Entrust Datacard keystore have OS layer protection of the keys. However, to ensure the integrity of the keys Entrust Datacard has added additional protection measures. Leveraging the security provided by mobile device operating systems, the Entrust Datacard Mobile Smart Credential 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 Datacard's solution design allows it to partner with the leading EMM and independent third party application vendors to ensure the proper integration with their applications and the Entrust Datacard Derived PIV Credential solution. These close relationships ensure both companies can support customer's 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 requires 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 Datacard Derived PIV Credential Solution can support LOA-4 enrollment, only the LOA-3 workflows will be presented in this document.

Issuance and Enrollment

Entrust Datacard has formed relationships with the leading EMM/MDM vendors who support Government and non-governmental agencies. These partnerships allow organizations to leverage their existing EMM/MDM investment for the deployment and ongoing management of the mobile devices and applications. For organizations who do not currently use an EMM/MDM solution the Entrust Datacard Mobile Smart Credential Solution can be effectively deployed and managed through our award winning Entrust IdentityGuard Authentication platform.

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 smartcard. By leveraging the Entrust Datacard self-service portal, PIV and CAC smart card users can request a Derived PIV Credential using their PIV or CAC smartcard for identity verification instead of having to go through a face-to-face identity verification process.

The Entrust Datacard 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, leading 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 IdentityGuard 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 7 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 IdentityGuard 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 Entrust Datacard Self Service Portal

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 employee's PIV Authentication certificate used to request the Derived PIV Credential. This will be their government email address. 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.

Derived PIV Credential Enrollment using the QR Code Option, one of four options available within the Entrust Datacard complete Derived PIV Credential Solution

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.

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 IdentityGuard 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 7 days after Derived PIV Credential issuance.

Once the employee has authenticated, they select the link to request a FIPS compliant One-Time Password (OTP). This OTP is delivered to the employee's government email. Using their mobile device, the employee navigates to the IdentityGuard 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.

LOA-3 enrollment on Blackberry for both COTS third party and native applications:

The Entrust Datacard Derived PIV Credential solution on Blackberry follows the same enrollment process as the Derived PIV Credential enrollment for third party COTS applications outlined above. The Entrust Datacard secure third party Derived PIV Credential keystore is directly integrated with the Blackberry trusted keystore, allowing the Derived PIV Credential to be available to all applications integrated with the Blackberry trusted keystore within the work partition. Unlike the iOS and Android platforms, both native and third party applications can leverage the Blackberry trusted keystore; eliminating the requirement for multiple Derived PIV Credentials to be enrolled on a single device to support both native and COTS third party applications.

Ongoing Management Self-Service Capabilities

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

The Entrust IdentityGuard 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 smartcard reader and request or manage their Derived PIV Credentials.

The Entrust IdentityGuard 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 IdentityGuard 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, US 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 smartcard, and securely protects against unauthorized users from logging into the IdentityGuard 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 on to their workstation or access services due to damage to their credential or being locked out caused by a forgotten PIN.

Unlike PIV smartcards, PIN unblock and reset is easily self-managed through both the Entrust IdentityGuard SSM and directly on the mobile device through the Entrust Mobile Smart Credential 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 Datacard solution's issuance and enrollment process also address 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 7 days after issuance
  - The Entrust Datacard 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 must be revoked
  - The Entrust Datacard PIV Credential Solution has fully available APIs for synchronizing the Derived PIV Credential revocation again PIV eligibility, ensure the solution is fully consistent with the standard without the need to expensive, one off customizations.

Issuing CA must be an authorized FED SSP for PKI

- Only the existing US Federal PIV providers are authorized to issue Derived PIV Credentials
  - Entrust Datacard is the only vendor that can provide a complete end-to-end Derived PIV Credential solution.

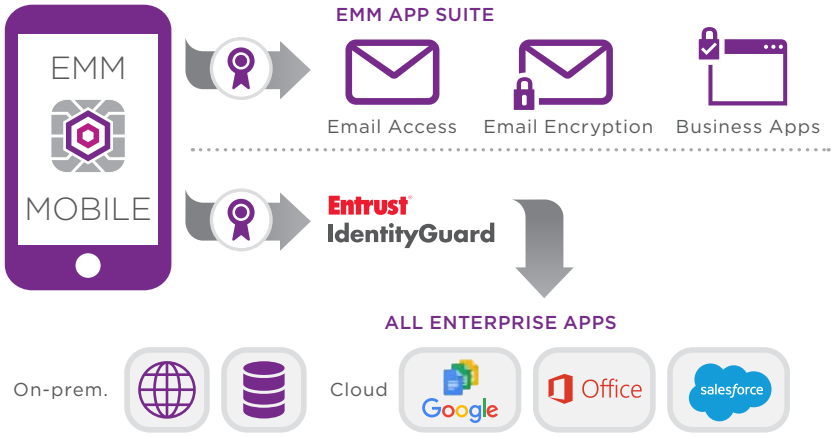
Shared Service Provider (SSP) CA Support

In addition to being able to provide the issuance, storage and use of the Derived PIV Credential, Entrust Datacard is an approved Federal Shared Service Provider (SSP) and fully supports the major US Federal SSP CAs used for PIV issuance. The Entrust IdentityGuard Mobile Smart Credential solution was developed to be able to consume certificates from the Entrust Federal SSP Certificate Authority. This puts Entrust Datacard in a unique position as being the only vendor in the marketplace to be able to provide a complete end-to-end Derived PIV Credential solution: enrollment and deployment of PIV compliant derived credentials to mobile devices, consumption and secure storage of NFI-SSP issued certificates, ongoing management and user self-management of their credential and integration with other key players in the mobile device and mobile application ecosystem. This ensures that Entrust Datacard can be relied on as a premier partner to meet today and tomorrow's mobile requirements.

Use Cases: Getting the Most out of your Mobile Smart Credential

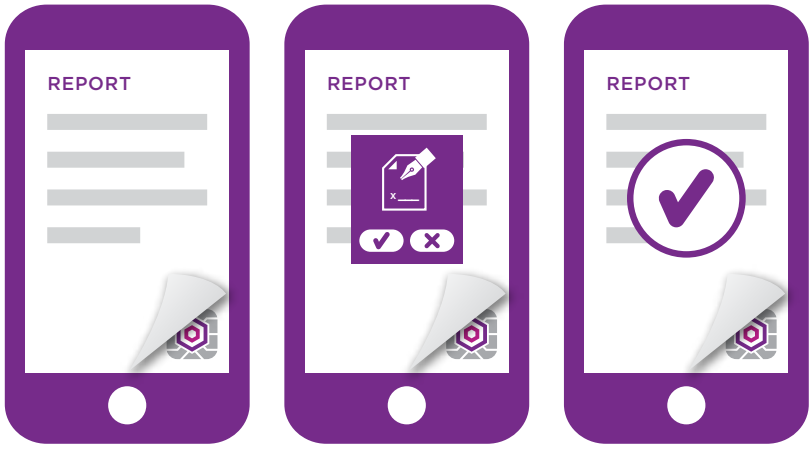
Once deployed the Entrust Datacard Mobile Derived PIV Credential allows mobile workers the ability to leverage their mobile devices to securely access information and complete transactions anytime, anywhere.

Accessing Web Applications



Whether it's a social worker helping clients, law enforcement needing information on a stopped driver or a manager requiring HR files while at home, having the information you need, when you need it can greatly improve productivity as well as accuracy in the service being provided. 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 Datacard addresses this issue in a number of ways to give organizations implementation flexibility. Through Entrust Datacard's integration with EMM 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, EMM integrated browser, or a specialized third party browser, the Entrust Datacard Derived Credential solution can issue and manage a Derived PIV Credential to meet the needs of an organization.

Digitally sign documents



User completes report

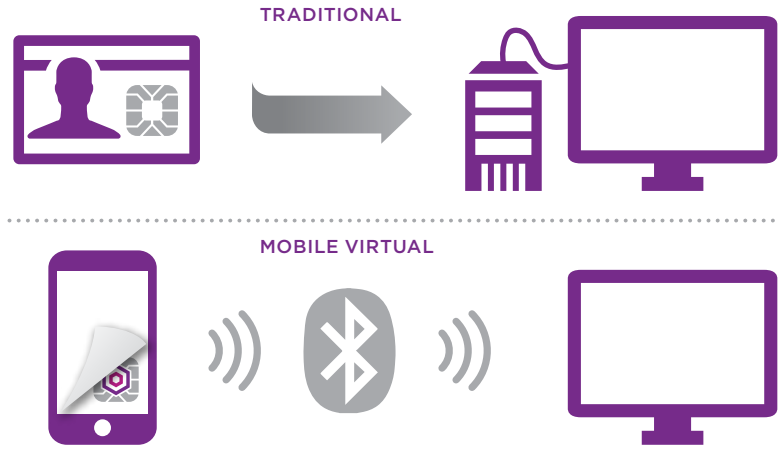
User promoted to digitally sign and submit report

User accepts and report is digitally signed using their Derived PIV Credential

When it comes to the mobile workforce, there are plenty of instances when work cannot be completed without the employee going back to the physical office. This takes time and eliminates the ability to provide on-demand, instant services. Because of Entrust Datacard Derived PIV Credential's ability to store and use signing certificates, through integration with digital signing applications, employees can digitally sign a request in the field. This means food inspectors could complete, sign and submit their reports in the field, contracts can be signed and filed from a hotel room, important services can be ordered while at a constituent's house, and police officers can request and receive a signed warrant without ever leaving a potential crime scene.

Automatically log on and off to Desktops

Entrust Datacard's derived credential provides a solution for both traditional smartcard log on 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 smartcard from the smart card reader to logoff. Often times 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.

Entrust Datacard Mobile Smart Credentials 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 Mobile Smart Credential is connected to a workstation, the mobile device operates much in the same way as a traditional physical smartcard. The Mobile Smart Credential continues to operate like a physical PIV smartcard; 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 smartcard logon experience that a user expects when using their PIV smartcard, reducing the amount of training required to use the derived Entrust Datacard Mobile Smart Credential.

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

If desired, Entrust Datacard'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 their 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 Datacard Derived PIV Credential it is important that it can integrate into an organizations existing application ecosystem.

Entrust Datacard has Technology Partnerships with key EMM vendors including MobileIron, Blackberry Good, VMware Airwatch and Citrix. These integrations allow the EMM 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's secure Sub Rosa reader application and Juniper Junos Pulse VPN client for PIV authentication to Web-based applications and web portals such as Microsoft Outlook Web Access (OWA), and Acronis for secure document retrieval and encryption.

Entrust Datacard also has a key integration with Monkton's Derived PIV Credential solution. This solution provides a streamlined method for enabling custom applications to leverage Derived PIV Credentials with less than 10 lines of code. This greatly reduces the complexities involved in developing organization specific custom applications, all the while ensure the solution is secure and consistent with the NIST SP 800-157 standard.

In addition, the Entrust Datacard Derived PIV Credential Solution has open APIs and SDK format lends itself to easy and direct integration with the Entrust Datacard solution. These various integration points ensure that the Entrust Datacard solution can meet the demands of any organization's mobile needs.

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, and gains secure access to information in the field and to complete transactions.

The HSPD12 / FIPS 201 Personal Identity Verification (PIV) program and NIST Specification 800-157 provides the framework to do this in a secure manner that protects both the employee and the customers they serve. Entrust Datacard solutions and the Entrust Mobile Smart Credential in conjunction with key partners provides agencies and supporting organizations the ability to implement a program that meets user needs while remaining compliant with federal regulations.

About Entrust Datacard

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

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

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA

Twitter Facebook Youtube LinkedIn Google+ RSS