MOBILE DERIVED PIV/CAC CREDENTIAL - A COMPLETE SOLUTION FOR NIST 800-157

Trusted Identities for Mobile as the New Desktop
# Table of contents

1. The Need for Mobile Derived Credentials  
   Page 3

2. Approval of the Mobile Derived Credential  
   Page 4

3. The First Complete Mobile Derived Credential Solution  
   Page 5

4. The Derived Credential Enrollment Process  
   Page 7

5. Challenges of Using Derived Credentials on Mobile Devices  
   Page 9

6. Use Cases & Authentication Methods  
   Page 10

7. Conclusion  
   Page 14
In an ever-reaching digital world, mobile is transforming businesses by providing employees with the freedom and ease of anytime, anywhere access to products, services and information. In this new, frictionless environment, employees are able to get their job done more efficiently than ever before—ultimately providing better customer service and competitive posture for businesses and organizations in a wide variety of markets.

As businesses make the move to mobile, digital identity is a key element to ensure authenticity of the users who access resources and conduct transactions. Unfortunately, traditional approaches to identity management do not align well with the mobile world. Usernames and passwords can be programmed into mobile devices for quick access, but they are insecure and inconvenient to reset. Stronger authentication methods that use solutions such as One Time Password (OTP) tokens can hinder the user experience and more streamlined methods such as smart cards simply can’t be inserted onto tablets and phones.

As US Government agencies establish plans to embrace mobile devices as alternatives to traditional desktop computers, special consideration must be given to ensure compliance with HSPD12 / FIPS 201 Personal Identity Verification (PIV) requirements. As such, NIST specification 800-157 outlines how PIV identities can be implemented and deployed directly on mobile devices. The mobile PIV credential is called a Derived PIV Credential.

The Entrust Mobile Derived Credential solution provides government agencies and contractors with a comprehensive, frictionless, and proven solution for placing Derived PIV Credentials onto mobile devices. Entrust Mobile Derived Credentials are easily accessed by employees and help harness the power of mobile as the new desktop by providing secure, anywhere anytime access to work files and systems.
Approval of the Mobile Derived Credential

With the publication of FIPS 201-2, the ability to place an HSPD-12-compliant credential onto a mobile platform became permissible as defined in the NIST Special Publication 800-157; this permissibility led to the development of Entrust’s mobile derived credential solution.

The ability to place the credential onto a mobile platform allows for greater flexibility for future Personal Identity Verification (PIV)-enabled applications and operations, as the traditional challenges of leveraging strong public key cryptography in mobile devices can be met by Derived PIV/Common Access Card (CAC) Credentials (derived credentials).

However, SP 800-157 stipulates that a derived credential can be self-managed by leveraging the strong identity binding associated with the PIV smartcard for the issuance of the derived credential. SP 800-157 allows the user to request their derived credential using their PIV smartcard instead of having to go through a face-to-face identity verification process.

In addition to meeting requirements for HSPD-12 enablement of mobile devices, derived credentials provide a backup credential for an employee whose PIV badge is lost or damaged. Complications could arise if smartcard logon (SCLO) is enabled for employees and their PIV badge is unavailable for use (e.g., forgotten PIN, damaged or lost smartcard). The user would be unable to log in to their workstation without first calling the helpdesk to enable password authentication for their account.

The end result in this scenario — particularly across large-scale agencies and organizations — demonstrates decreasing productivity and security, and increasing administrative costs. Helpdesk calls can be avoided if employees are issued derived credentials, which may be used for SCLO in place of their PIV credential.

This is especially helpful to remote employees or staff who may not have easy access to a PIV enrollment center (e.g., employees deployed overseas).

Deriving Trust from Bound Identities
The trust for the new credential is derived by the strong identity binding associated with the authenticated PIV smartcard during enrollment.

It is important to note that only the trust is derived during enrollment; the Derived PIV certificates themselves are cryptographically unique from the user’s PIV credentials. After issuance, the PIV smartcard could be revoked or replaced without affecting the trust of the derived credential. This is similar to how an individual applies for a passport using the trust of another government-issued credential, such as their driver’s license. Once issued, their passport does not require replacement if their license expires or is revoked.
Recognizing the importance of NIST SP 800-157, Entrust developed its Mobile Smart Credential Application (MSC) as a full-featured, enterprise-ready solution for the derived credential. The Entrust IdentityGuard Mobile Smart Credential is available for use on Apple iOS, Google Android and BlackBerry mobile operating systems.

The Entrust IdentityGuard Mobile Smart Credential application 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 the same certificate types and use the same communication language traditionally used on a physical PIV smartcard.

This results in greater interoperability with existing PIV-enabled websites and applications. The PIV-enabled application views the Mobile Smart Credential in the same way it would interact with a traditional PIV smartcard.

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

**Self-Service Capabilities**

In comparison to other derived credential solutions, Entrust IdentityGuard is unique in its ability to provide a Self-Service Module (SSM); granting users’ access to request and manage their Derived PIV Credentials without the need for administrative interaction. The SSM fully leverages the advantages provided by SP 800-157, and greatly reduces the administrative costs associated with other derived credential solutions.

The Entrust IdentityGuard SSM is accessed through a Web-based interface and can be deployed in a high-availability architecture, which greatly increases scalability and reliability, as only a few servers could be deployed locally to service users around the world.

This approach helps reduce operational costs by limiting the need to deploy specialized enrollment stations and kiosks abroad for derived credential enrollment. Users would be able to access the SSM from any workstation with a working smartcard reader and be able to request or manage their derived credentials.
PIN Unlock, Reset via SSM
Due to the unique missions across the US Federal space, many employees are often deployed away from their department’s PIV enrollment offices. Having a secondary HSPD-12 credential that is easily and securely self-managed, reduces the likelihood of a deployed employee from being unable to log on to their workstation due to damage or lockout 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. With this solution, there is no need for a specialized kiosk for derived credential issuance and management.

If policy does not allow for users to unlock or reset their derived credential PIN, or if the user loses their mobile device, the SSM allows for the old derived credential to be quickly suspended or revoked. The user would enroll for a new derived credential on their new or existing mobile device.

In addition to being able to provide the issuance, storage and use of the Derived PIV Credential, Entrust is an approved Federal Shared Service Provider (SSP) and can issue the certificates themselves. The Entrust Federal SSP Certificate Authority integrates seamlessly with the Entrust IdentityGuard Mobile Smart Credential solution. This puts Entrust 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: from registration, authentication, PIV certificate validation and issuance to the mobile device, secure storage and use of the Derived PIV credential.
To request and enroll a Derived PIV credential on the Entrust IdentityGuard Mobile Smart Credential application on a mobile device, the user navigates to the Entrust IdentityGuard SSM through their Web browser on their workstation. The user authenticates to the SSM using their physical PIV smartcard, granting them access to request their mobile credential. By authenticating to the SSM with their PIV smartcard, the user establishes the first assertion of their identity to the issuance of their derived credential. This initial login can also be locked down to accept only PIV or CAC OID’s.

After the SSM validates the user’s PIV smartcard credential – checking for PIV or CAC policy OID’s as well as checking the validity of the authentication certificate via a Certificate Revocation List (CRL) or an Online Certificate Status Protocol (OCSP) - the user selects the link to request a derived credential.

Next, Entrust IdentityGuard can be configured for several different Derived PIV Credential activation methods, providing the most flexible solution to meet the needs of various policies and requirements. These activation methods include:

a) QR Code with password displayed. Activation information is encoded in a QR code displayed on the Entrust IdentityGuard Self-Service Web page, along with the password needed to unlock the information. The option to print out the QR code is also available.

The user opens the Entrust Mobile Smart Credential Application on their mobile device, captures the QR code, and enters in the password. This decrypts the information, allowing the user to generate and activate their Derived PIV Credential.

b) QR Code with password via encrypted email. Activation information is encoded in a QR code displayed on the Self-Service Web page, and the password you need to unlock the information is sent to you in an encrypted email. The email is encrypted using the PIV encryption credentials found on the user’s PIV smart card. The option to print out the QR code is also available.

The user opens the Entrust Mobile Smart Credential Application on their mobile device, captures the QR code, and enters in the password. This decrypts the information, allowing the user to generate and activate their Derived PIV Credential.
c) Email with password displayed. A password-protected activation link is sent to the user in an email and the Self-Service Web page displays the password needed to unlock the link.

The user clicks on the activation link, it opens the Entrust Mobile Smart Credential Application on their mobile device. The user enters in the password displayed on the Self-Service Web page. This decrypts the link, allowing the user to generate and activate their Derived PIV Credential.

d) Email with password via encrypted email. A password-protected activation link is sent in one email, and the password needed to unlock the link is sent in a second encrypted email.

Email 1: The first of these two emails is sent unencrypted and contains a link back to the Self-Service Web page for issuance of the derived credential. This email contains an encrypted link that can only be decrypted using the password delivered in Email 2.

Email 2: The second email is encrypted and contains a password that must be used on the mobile device to log in to the Entrust IdentityGuard Self-Service Web page for derived credential issuance. This second email is encrypted using the user’s encryption PIV credentials found on their PIV smartcard.

The user opens Email 1 on their mobile device, clicks on the link, and enters the password from Email 2 and generates and activates their Derived PIV Credential.

These various activation options provide multiple, secure workflows for allowing a user to generate and activate their Derived PIV Credential. These activation options provide the flexibility required to comply with the various security policies and technical challenges encountered by many of the US Federal Departments and Agencies. The result is a turn-key experience, reducing deployment and architecture costs.
Challenges of Using Derived Credentials on Mobile Devices

One of the main challenges of using derived credentials on mobile devices is actually the result of one of the strengths in the mobile architecture. Applications on a mobile device are installed independently of other mobile applications. Each mobile application exists in a virtual sandbox, separated from the other applications installed on the same device. This is contrary to the shared memory space of a traditional desktop computer.

At the time of publication, there are no known exploits that can penetrate this sandbox for an unauthorized application to gain access to other installed applications. For this reason, mobile applications can often be made more secure than their traditional desktop counterparts.

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

Building On the Security of the Sandbox

To further add to the security provided by mobile device operating systems, the Entrust 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, if higher levels of assurance and security are required, the Entrust Mobile Smart Credential application in the future will support the use mobile device hardware, i.e. trusted execution environment and secure element.
Use Cases & Authentication Methods

There are two main ways a derived credential could be leveraged to increase security. The first is to provide access to certificate-enabled mobile applications for authentication directly through the mobile device – removing the need for username and password. This increases the flexibility for employee access to applications via mobile devices while maintaining the level of security provided by secure PIV authentication for application access through the mobile device.

The second is to use the derived credential to provide logical access to a traditional workstation or laptop; similar in how a PIV smartcard is used for SCLO. This can then be used as an alternative authentication method to the desktop and network should the user’s PIV card be lost or damaged.

An advantage of the Entrust Mobile Smart Credential application is that both methods of access can be easily configured, and are enhanced through Entrust partnerships with other leaders in the mobile device industry. Additionally, flexible and easy-to-use API’s provide the ability to build authentication into custom agency applications as well, which provides an off-the-shelf solution for enterprise deployment.

Mobile Authentication

Having a derived PIV credential on your mobile device provides no value to a user or an Agency unless that credential can be used to access agency resources and applications. With the Entrust Derived PIV credential solution, users are able to use their derived credential to authenticate directly to PIV-enabled applications through their mobile device. This is accomplished through various technology partnerships which continues to grow and expand.

By integrating the Entrust Mobile Smart Credential with Thursby’s secure PkardPro reader application, the derived credentials are able to be used for authentication to all Web-based applications and web portals accessible by the mobile device. Additionally, for those web applications and web portals that use a PIV for authentication today, this capability is enabled with no change to the existing infrastructure. (NOTE – traditional mobile device web browsers will not work as they do not support client side PKI authentication).

This integration provides a wide range of access, including PIV authentication to Juniper Junos Pulse VPN client, and other protected Web-based applications such as Microsoft Outlook Web Access (OWA). This integration is also extended to other applications, including Acronis and Silanis. Acronis provides secure document retrieval and encryption; Silanis will apply digital signatures to documents from a mobile device. Other integrations include Mobile Iron, Good, Blackberry, Citrix and others.
An example use case for the power and value of the above integrations might be a traveling executive, who is not connected to his corporate intranet, may quickly and securely provide a trusted digital signature to a document from a mobile device. This user may even email that signed document to the necessary parties, greatly reducing the delay in document approval often encountered when a traditional workstation is unavailable.

This type of quick document approval is invaluable when unexpected deadlines are encountered and swift responses are required.

Entrust’s derived credential offers simple integration with many leading applications — either directly through the mobile device or via smartcard logon from a traditional workstation.
Desktop Authentication – PIV alternative
The Entrust Mobile Smart Credential can be securely connected to a traditional workstation or laptop through a secure Bluetooth or NFC connection depending upon the devices used.

The Bluetooth connection is further secured through the use of AES 256-bit session keys, and a public/private 2048-bit key pairing unique to the mobile device or workstation pairing. A unique key pair is securely generated for each new workstation the Mobile Smart Credential is paired with, further strengthening the security of the connection.

A Familiar Smartcard Experience
When the Entrust Mobile Smart Credential is connected to a workstation, the mobile device operates much in the same way as a traditional physical smartcard. This provides the same smartcard log on experience that a user expects when using their PIV smartcard, reducing the amount of training required to use the derived Entrust Mobile Smart Credential.

Once logged on to their workstation, 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 provides seamless integration with existing PIV-enabled applications such as the Microsoft Office suite, including Outlook.
Automatic Desktop Locking
If desired, Entrust’s derived credential also supports automatic locking of the Microsoft Windows operating system if the smart credential is disconnected from the workstation.

Enabling this policy locks the user’s workstation when their mobile device is taken out of range from their workstation. This range is configurable.

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 the sensitive networks. This also reduces the likelihood of users leaving their credential in the reader when they walk away, as users generally are more mindful to remember their mobile device than they are to remove their PIV smartcard from a card reader.

US Federal Shared Service Provider Certificate Authority Support
Entrust IdentityGuard fully supports the major US Federal SSP CAs used for PIV issuance. This allows Entrust IdentityGuard to issue certificates containing the federally approved Derived Credential OIDs.

Certificate Policy OIDs
Entrust IdentityGuard can be configured to require the PKI credential used to log into the User Self Service Module to be issued by a registered US Federal SSP CA. Additionally, the Entrust IdentityGuard system can required 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 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.

Fully-Realized Security Solutions
Entrust Datacard also offers multiple solutions to help issue and manage highly secure identities and transactions. In addition to offering advanced document issuing printers that can produce electronic, personalized smart cards that are FIPS-201 certified, Entrust Datacard has the ability to issue Entrust Digital and SSL Certificates from the Shared Service Provider (SSP), a Certificate Management System (CMS) that is also FIPS-201 compliant.
As U.S. federal agencies continue to investigate their options to bring standard enterprise and mission-critical applications securely to employees’ mobile devices, the Entrust Mobile Smart Credential solution is highly attractive to enterprise road warriors, field workers and government organizations that require high assurance trusted IDS. By partnering with key technology players, Entrust Datacard supports and solves some of the most commonly requested use cases in a variety of government agencies at many different levels with the Entrust IdentityGuard Mobile Derived Credential solution that is ready for deployment today.

Conclusion
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@entrust.com or visit www.entrust.com.

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA