Deriving a Trusted Mobile Identity from an Existing Credential

Exploring and applying real-world use cases for mobile-derived credentials
# Table of contents

1. Approval of the mobile-derived credential  
   Page 3

2. The first complete mobile-derived credential solution  
   Page 4

3. The derived credential enrollment Process  
   Page 5

4. Challenges: Derived credentials on mobile devices  
   Page 6

5. Use cases & authentication methods  
   Page 8

6. Conclusion  
   Page 11
Approval of the mobile-derived credential

Advanced self-management greatly reduces the administrative overhead required for the issuance and maintenance of derived credentials.

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 draft NIST Special Publication 800-157.

This allows for greater flexibility for future PIV-enabled applications and operations, as the traditional challenges of leveraging strong public key cryptography in mobile devices can be met by derived credentials. Currently, NIST SP 800-157 describes how to issue a mobile-derived PIV credential then use it with mobile applications. Specifically, this outlines PIV authentication from a mobile device to an agency’s corporate intranet.

In addition to HSPD-12 enablement of mobile devices, derived credentials provide a backup credential for an employee whose PIV badge is lost or damaged. This is helpful to remote employees, or staff who may not have easy access to a PIV enrollment center (e.g., employees deployed overseas).

Reduce Costs, Maintain Security

Complications could arise if smartcard logon (SCLO) is enabled for these employees and their PIV badge is unavailable for use (e.g., forgotten PIN, damaged or lost smartcard). The user would be unable to log on to their workstation without first calling the helpdesk to enable password authentication for their account.

The end result in this scenario — particularly when scaled across large-scale agencies and organizations — demonstrates the decrease of productivity and security, and increases in 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.

SP 800-157 provides the ability for the derived credential to be self-issued by leveraging the strong identity binding associated with the PIV smartcard for issuance of the derived credential. This 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.

Leverage Identity-Proofing from Existing Vetted PIV Identities

The identity proof 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 existing vetted PIV identity is leveraged during enrollment; 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 in 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.

Self-Service Capabilities

In comparison to other derived credential solutions, Entrust IdentityGuard is unique in its ability to provide a self-service module; granting access for a user to request and manage their derived credentials without the need for administrative interaction. This fully leverages the advantages provided by SP 800-157, and greatly reduces the administrative costs associated with other derived credential solutions.

The Entrust IdentityGuard self-service module (SSM) is accessed through a Web-based interface and can be deployed in a high-availability architecture. This 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.
The derived credential enrollment process

1. To request and enroll a derived credential on the Mobile Smart Credential through Entrust IdentityGuard, the user navigates to the Entrust IdentityGuard Self-Service Module (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 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.

2. After the SSM validates the user’s PIV smartcard credential, the user selects the link to request a derived credential.

3. Next, Entrust IdentityGuard sends two emails to the user, using the email address found in the user’s PIV certificates on their smartcard. These emails allow the user to securely log in to the SSM through their mobile device, where attaching and using their physical PIV smartcard for authentication is not feasible.

   **Email 1:** The first of these two emails is sent unencrypted and contains a link back to the SSM for issuance of their derived credential.

   **Email 2:** The second email is encrypted and contains a cryptographically unique one-time-passcode (OTP) that is used on the mobile device to complete enrollment for the derived credential. This second email is encrypted using the user’s PIV credentials found on their PIV smartcard.

4. To gain access to the SSM on their mobile device, the user is required to decrypt the second email using their PIV smartcard.

5. The user navigates to the link identified in the first email through their browser on their mobile device and authenticates into the SSM using the one-time-passcode decrypted from the second email.

6. The user selects the link to activate their derived credential, which begins the enrollment process onto their mobile device.
Challenges: 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.

For mobile devices with updated operating systems, there are no known exploits at the time of publication 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.

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, a future release of the Mobile Smart Credential application will support the use of a secure element and Trusted Execution Environment (TEE).
However, due to this sandboxed environment, it is very difficult to allow a mobile application to be accessed by other applications — both on and off the device — without a special binding. This could greatly complicate using a derived credential, as PIV-enabled applications would be unable to access the cryptographic keys stored on the mobile device.

For any derived credential solution to be successful, the credentials stored on the mobile devices need to be made readily available, in a secure manner, to those applications requiring PIV authentication.

Additionally, there are two main ways a derived credential could be leveraged. The first 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.

The second is to provide access to PIV-enabled applications directly through the mobile device. A good derived credential solution should provide both methods of access. This tactic increases the flexibility for employee logical access and maintains the level of security provided by secure PIV authentication, encryption and digital signatures, as described in FIPS 201.

An advantage of the Entrust MSC application is that solutions to these challenges are available within the product, and further enhanced through Entrust partnerships with other leaders in the mobile device industry. This presents an off-the-shelf solution for enterprise deployment.
As mentioned, 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.

Entrust’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.

**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.

PIN Unlock, Reset via SSM
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 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.
Third-Party Integration Enhances Mobile Authentication

Besides using the Entrust Mobile Smart Credential as an alternative smartcard logon for their workstation, users could use their derived credential to authenticate directly to PIV-enabled applications through their mobile device. This is accomplished through a partnership with Thursby.

By integrating the Entrust Mobile Smart Credential with Thursby’s secure PkardPro reader app, the derived credentials are made available to all Web-based applications accessible by the mobile device. This occurs much in the same way existing Web-based applications leverage MS CAPI for PIV authentication on physical workstations.

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), or your Web single sign-on (SSO) product.

By leveraging the integration with Thursby, the Entrust Mobile Smart Credential is securely accessible for many other applications, including Acronis and Silanis. These applications provide secure document retrieval and encryption, as well apply digital signatures from a mobile device. Authentication with the Entrust Federation Module will provide users with SSO capability to SAML-based Web applications.

For example, executives who are traveling and not connected to their 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.
Conclusion

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. By partnering with such technology players as Thursby (and their ecosystem of partners), Entrust supports and solves some of the most commonly requested use cases in a variety of government agencies at many different levels.
Entrust offers software authentication platforms that strengthen security in a wide range of identity and transaction ecosystems. Government agencies, financial institutions and other enterprises rely on Entrust solutions to strengthen trust and reduce complexity for consumers, citizens and employees.

Now, as part of Datacard Group, Entrust offers an expanded portfolio of solutions across more than 150 countries. Together, Datacard Group and Entrust issue more than 10 million secure identities every day, manage billions of secure transactions annually and issue a majority of the world’s financial cards.

For more information about Entrust solutions, call +1 888-690-2424, email entrust@entrust.com or visit www.entrust.com.

Company Facts
Website: 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