MobileIron Derived Credentials with Entrust

Overview

Government agencies have very stringent security regulations. Agencies protect their information systems, in part, by limiting access to the minimum set of users required to perform a function. This principle of "least privilege" requires both authentication and authorization processes. Federal Information Processing Standards (FIPS) Publication 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors mandates using smart cards to provide two-factor authentication for access to federal information systems.

These standards address the requirements for initial identity proofing, infrastructures to support interoperability of identity credentials, and accreditation of organizations and processes issuing PIV credentials. They worked great for laptops and desktop computers, which were the preferred devices to access federally controlled information systems and applications. But the device landscape has changed significantly now.

Mobile devices have become ubiquitous and has become the defacto device of choice to access federal applications, including email. Their form factor and UX is very different from traditional desktops and laptops and that makes them very hard to use with card readers. Attaching or tethering a separate external smart card reader to mobile phones or tablets creates usability and portability challenges and makes the smart card an impractical authentication token, besides adding additional costs and complexities of the middleware. Agencies reliant on smart-card-and-password two-factor authentication are requiring even more stringent secured credentials can now leverage CBA (Certificate based authentication) to authenticate users of mobile devices in a way that is more tamper-resistant than a password, and as easy to use as a smart card.

Solution

MobileIron has worked with Entrust to create a Derived Credential solution that will enable government agencies to extend their existing security investments, such as common access cards (CAC), and personal identity verification (PIV), to give mobile devices secure access to agency resources without requiring employees to use additional hardware like sleds or smart card readers. The solution is compliant with government regulations and security standards such as Homeland Security Presidential Directive-12 (HSPD-12), Federal ICAM initiatives, FIPS 201 and NIST SP:800-157.

The solution can be implemented in 6 easy steps:

The derived credential is created on the device directly and not transferred to/from any other location. This ensures that the credentials are never tampered with nor can they be transferred to any other device.

1. IT administrator at the agency sets up the infrastructure with MobileIron and Entrust.
2. User logs into the MobileIron Self Service portal from a PIV registered laptop/desktop.
3. User initiates and completes the device registration.
4. User then logs onto the Entrust Identity Guard Self Service Module from the laptop to enroll a derived mobile smart credential.
5. User launches the new MobileIron PIV-D Entrust app and activates PIV-D using a PIN number. This generates the credential on the device directly.
6. User can then access all AppConnect applications on their mobile device (i.e. email, web browser, file shares, etc.) by using the credential which was derived from their physical PIV card and protected by a secure AppConnect container with FIPS 140-2 encryption.

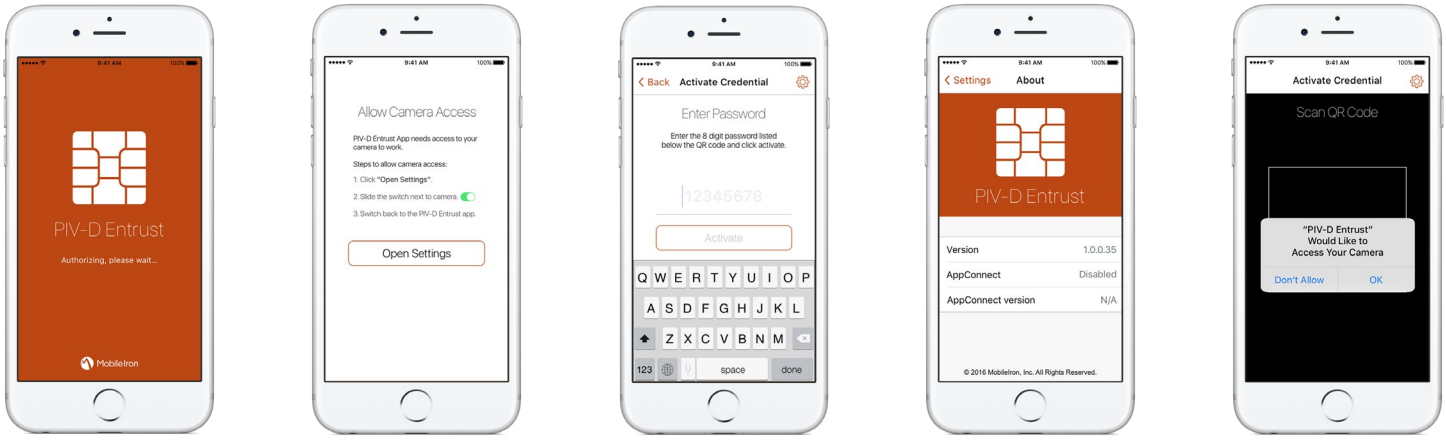
MobileIron

Benefits of MobileIron solution with Entrust

The MobileIron Derived Credentials solution with Entrust ensures the highest levels of security while not compromising the user experience of the end user. The same level of security provided by PIV cards is extended to mobile devices and by generating the credentials directly on the device, the integrity of the credentials is maintained. The credentials are also protected by the AppConnect encryption and compliant with NIST SP 800-157. The solution allows agencies to provide the best user experience for all their users, when they access critical agency resources such as email and sensitive applications from their mobile devices. Most importantly this 1st to market PIV-D (800-157 derived credential) will become the first step in eliminating the risks and vulnerabilities of passwords and usernames.

> *"CAC cards can still be used to get into a building, but we will not use them on our information systems. True multi-factor authentication will make us more agile and cut the cost overhead."*
>
> **- Terry Halvorsen, DoD Chief Information Officer**
>
> *http://federalnewsradio.com/defense/2016/06/dod-plans-bring-cac-cards-end/*

MobileIron is the only EMM provider with all Federal certifications, including 3rd party accredited FIPS 140-2, NIAP MDMPP v2.0 Common Criteria certification, DISA STIG approval and has achieved FedRAMP authorized status. With such strong security focus, MobileIron is the leading provider of EMM solutions to Federal agencies worldwide.



For More Information, please visit

https://www.mobileiron.com/government or contact us at globalsales@mobileiron.com.

MobileIron

415 East Middlefield Road, Mountain View, CA 94043

info@mobileiron.com | www.mobileiron.com

Tel: +1.877.819.3451 Fax :+1.650.919.8006