VMWARE AIRWATCH DERIVED CREDENTIALS FOR EMM

Enabling Two-Factor Authentication on Mobile Devices

OVERVIEW

The VMware AirWatch® derived credentials solution provides the highest level of security for mobile devices for both native and third-party applications.

KEY BENEFITS

- Provides two-factor authentication for mobile devices without the need for awkward hardware attachments.
- Allows government agencies to leverage current security investments.
- Integrates with several leading Credential Management solutions, including XTEC, Entrust, Microsoft and more.

The Need for Derived Credentials

Smart card authentication has been the de facto standard within the US Federal Government since the early 2000's, specifically with the issuance of FIPS 201 by the National Institute of Standards and Technology (NIST). Both the Department of Defense (DoD) as well as all Federal Civilian agencies must utilize smart cards for physical, logical, and network access. The DoD utilizes a Common Access Card where as their civilian counterparts utilize a Personal Identification Verification (PIV) card.

At the time that FIPS 201 was introduced and mandated, the standard operating environment consisted primarily of desktops and laptops. Smart card integration with laptops and desktops is fairly trivial, as the laptops have built-in smart card readers, and the desktops utilize USB-based smart card readers. Also, these desktops and laptops support smart cards at the operating system level, so any application that runs on the operating system can take advantage of the smart card. More recently, however, the proliferation of mobile devices as the primary method to access Federally-controlled information systems and applications has created a need to change the way we authenticate. Integrating or attaching additional hardware onto the small form factor of a mobile device is costly, cumbersome, and simply not practical. To help solve this problem, NIST updated FIPS 201 to include additional form factors and in 2014, NIST released a special publication (800-157) titled "Guidelines for Derived Personal Identification Verification (PIV) Credentials." Instead of utilizing the CAC or PIV Card, this special publication provides the guidelines for how to generate and utilize an alternative token, which can be implemented and deployed directly with mobile devices. This newly derived PIV credential is also commonly referred to as a derived credential or PIV-D.

Enabling Mobility with Derived Credential Support Using AirWatch

From an industry perspective, derived credentials is still a very new concept, which means there are numerous vendors and approaches without a real reference implementation. One of the key challenges that agencies will face when choosing the right solution is to decide whether they want to focus on integration with native OS-provided applications or third-party custom SDK-enabled applications.

LEARN MORE

For more information on AirWatch EMM capabilities for high security environments, visit http://www.air-watch.com/industries/federal-government

VISIT

Visit the National Institute of Standards and Technology for more information. http://www.nist.gov

AirWatch's approach to derived credentials solves this challenge by providing a holistic solution that allows agencies to utilize the derived credential for both native and third-party applications. This mitigates the need for government agencies to utilize hardware-based smart card readers that are often referred to as sleds. Our approach derives the credential and stores it in a hardware backed keystore that the underlying operating system provides which complies with NIAP and NSA guidance. The credential is then secured using an authentication PIN or biometric input, and leveraged by the mobile device to be used by work applications (native or third-party) to authenticate the user in lieu of the physical CAC/PIV card connected to the mobile device. The solution features an identity technology allowing certificate authentication to be added to existing software applications without rewriting or investing in building certificate authentication directly into each application.

This approach gives organizations the ability to integrate with various industry-leading Credential Management solutions in the market including Entrust, XTEC, Microsoft ADCS, Intercede and many others. Ongoing compliance, user auditing and remediation are done automatically from the AirWatch platform.

AirWatch helps many federal, financial service, energy and other heavily regulated security-conscious industries and agencies comply with their information assurance requirements while still meeting demands of their mobile use cases. Various other certifications and standards including FIPS 140-2, FedRAMP Certification, SOC 2 Type 2 compliance and others have been obtained including a STIG for both iOS and Android from the Defense Information Systems Agency (DISA).

vmware® airwatch®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com