VMware Workspace ONE PIV-D Manager

Derived credentials for two-factor authentication on mobile devices

OVERVIEW

VMware Workspace ONE® PIV-D Manager 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 U.S. federal government since the early 2000s, 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 (CAC), whereas 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: Laptops have built-in smart-card readers, and desktops utilize USB-based smart-card readers. Also, these desktops and laptops support smart cards at the OS level, so any application that runs on the OS can take advantage of the smart card.

More recently, 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 released Special Publication 800-157, "Guidelines for Derived Personal Identification Verification (PIV) Credentials," in 2014. Instead of utilizing the CAC or PIV card, these guidelines detail how to generate and utilize an alternative token that 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.

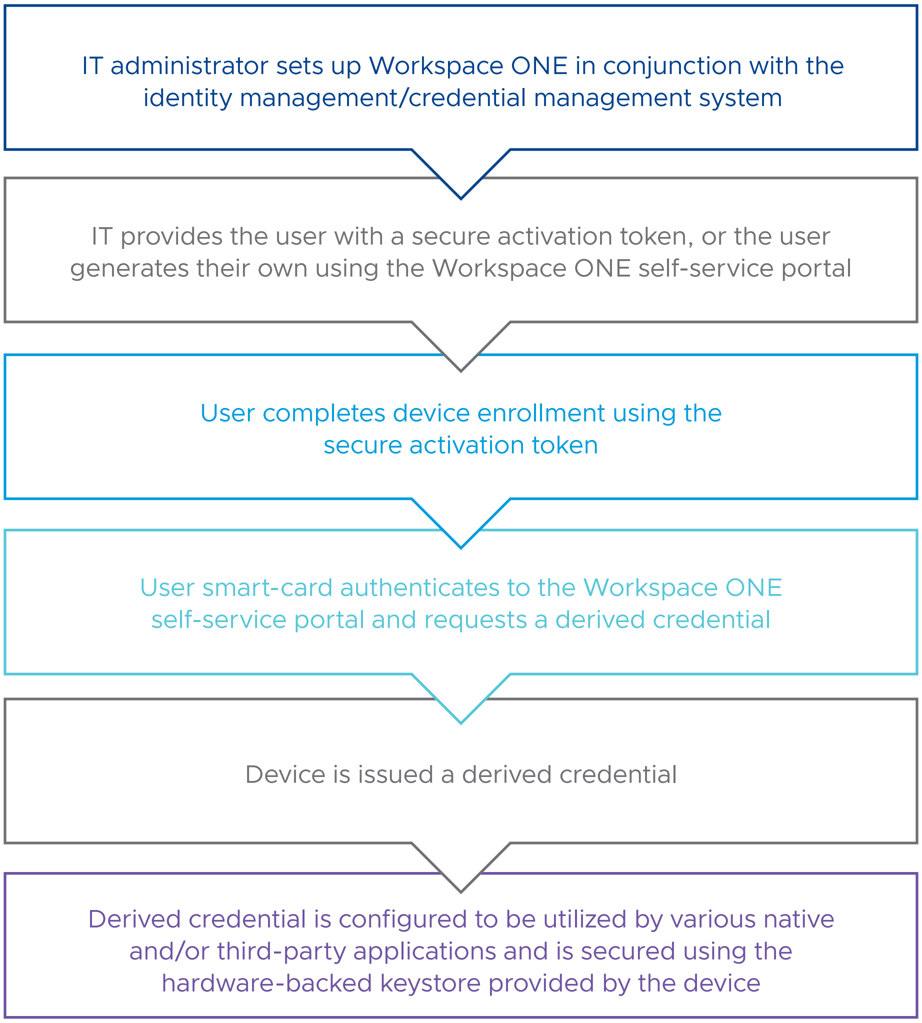
Enabling mobility with derived credential support using Workspace ONE

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 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.

The VMware Workspace ONE 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, often referred to as sleds.

Our approach derives the credential and stores it in a hardware-backed keystore that the underlying OS provides, which complies with guidance from the National Information Assurance Partnership (NIAP) and the National Security Agency (NSA). 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. Workspace ONE can easily set up the derived credential solution, as shown in Figure 1.



IT administrator sets up Workspace ONE in conjunction with the identity management/credential management system

IT provides the user with a secure activation token, or the user generates their own using the Workspace ONE self-service portal

User completes device enrollment using the secure activation token

User smart-card authenticates to the Workspace ONE self-service portal and requests a derived credential

Device is issued a derived credential

Derived credential is configured to be utilized by various native and/or third-party applications and is secured using the hardware-backed keystore provided by the device

FIGURE 1: Workspace ONE methodology for setting up derived credentials.

This approach gives organizations the ability to integrate with various industry-leading credential management solutions in the market, including Entrust, XTec, Microsoft Active Directory Certificate Services (ADCS), Intercede, and many others. The Workspace ONE platform automatically performs ongoing compliance, user auditing, and remediation.

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

LEARN MORE

For more information on the VMware Workspace ONE capabilities for high security environments, visit *https://www.vmware.com/solutions/industry/government/federal-government-it-solutions.html*.

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

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