ENTRUST IDENTITY ENTERPRISE AND VMWARE WORKSPACE ONE

Building Strong Alliances for an Integrated Mobile Identity Assurance Solution

Secure your mobile workforce with a derived PIV credential solution

The Problem

Smart cards on mobile devices are incredibly limited

We live in a world that demands anytime, anywhere access. To satisfy these demands in an environment that presents a very broad and dynamic threat landscape, authentication solutions must evolve quickly. As threats, capabilities, and technology continue to evolve, the solutions we turn to for digital trust must protect, but also enable, a drive toward improved business outcomes through streamlined access mechanisms.

Directives like HSPD-12 and FIPS 201 mandate that smart cards (i.e., CAC and PIV) be used for all physical, logical, and network access. Unfortunately, these directives were made before the introduction of mobile devices. As a result, the integration of smart card readers with mobile devices has been largely unsuccessful. These readers are expensive and bulky, and their clunky designs clash with the intuitive design of mobile devices.

In other words, just because it's labeled smart, there is no guarantee that it is smart or will provide a secure, seamless experience.

KEY BENEFITS

- Anytime, anywhere secure access to applications, resources, and information
- Deploy and manage existing and new mobile devices and applications
- Leverage existing smart card/PIV deployment to derive a strong, mobile-based user credential bound to their device
- Pre-integrated with EMM to reduce IT cost and complexity
- Flexible deployment: on-premises or fully-managed cloud service

Workspace ONE

Learn more about our IAM solutions at Entrust.com

Entrust and VMware integrated derived PIV credential solution

The Challenge

Accelerating the adoption of secure technologies

As federal agencies and enterprises continue to go digital, mobile technologies are widely recognized as the primary enabler for optimizing productivity, transforming service delivery, and reducing overhead. Mobile-first models are being adopted more and more, making access to sensitive data a very important consideration.

The Federal HSPD-12/FIPS 201-2 Personal Identity Verification (PIV) program mandates smart card authentication to ensure the integrity of both data and the individuals accessing that data. Since government agencies and other industries want to use mobile technologies that protect sensitive data while eliminating the need for passwords and hardware tokens, there is a desperate need for a best-in-class solution.

The Solution

A collaboration of innovators providing real-world, standards-based cybersecurity

Entrust certificate-based, mobile smart credential technology, combined with VMware® Workspace ONE, provides secure access to mobile users while minimizing factors and friction.

This integrated derived PIV credential solution establishes secure remote access to your networks and applications via certificate-based authentication. This allows your mobile workforce, remote and branch offices, and remotely connecting partners and clients to safely access your services using their mobile devices – all in a way that is compliant with U.S. Federal HSPD-12/FIPS 201-2 PIV program mandates – and replaces workstation smart card reader access.

Primary use cases

- Mobile authentication, signing, and encryption
  - Native applications and profiles (VPN, secure email, secure browsing)
  - Third-party applications
  - NIST SP 800-157 compliant
- Replace existing smart cards by transforming mobile into a virtual smart card to streamline workstation authentication for:
  - Workstation smart card logon
  - Two-factor authentication for VPN, on-premises, and cloud apps
  - Email encryption and digital signing

Learn more about our IAM solutions at Entrust.com

Entrust and VMware integrated derived PIV credential solution

Why use Entrust Identity Enterprise and VMware Workspace ONE?

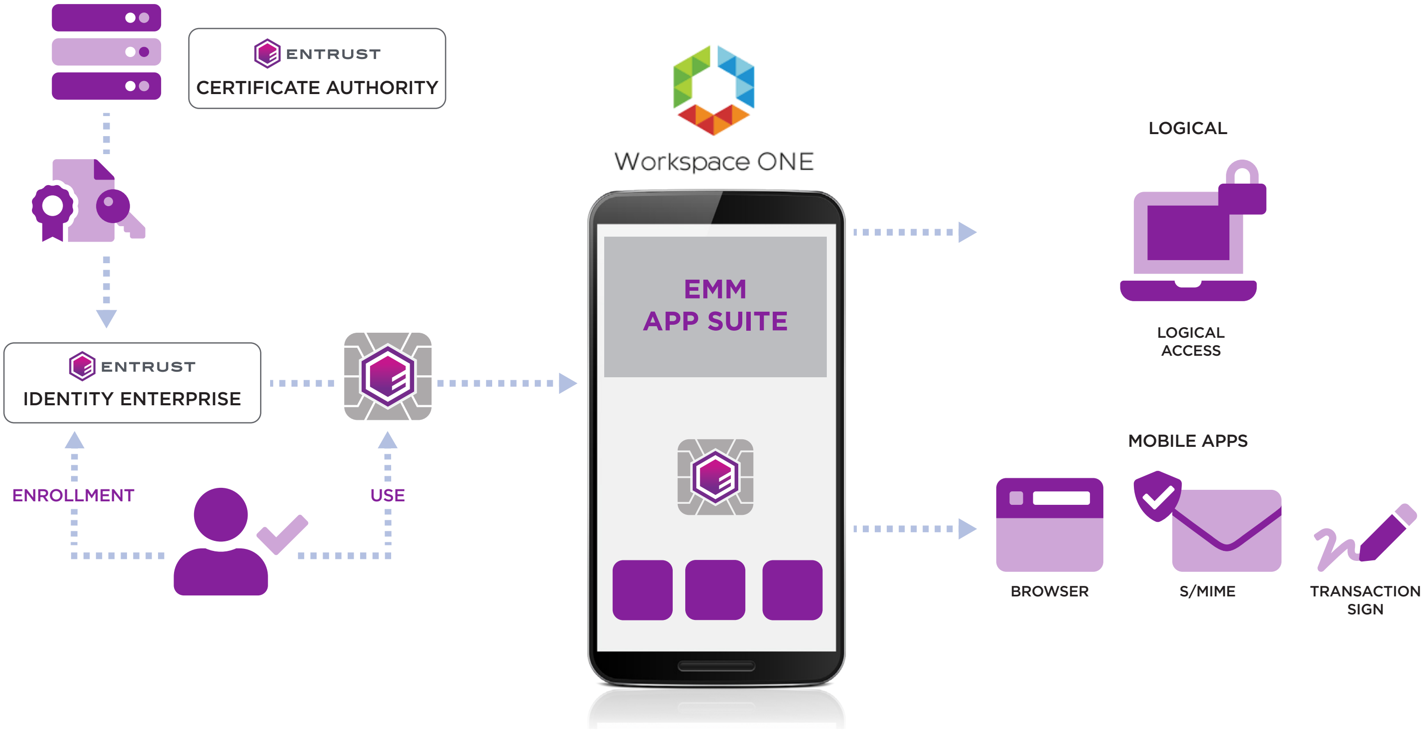
When you provide mobile employees trusted identities to complete secure transactions all through a seamless user experience, you not only maximize valuable resources, you optimize the usefulness of trusted identities. While federal mandates serve as a catalyst for the use of derived credentials, the solution outcome and methodology are directly relevant to any organization moving to more secure forms of authentication.

The Entrust and VMware® Workspace ONE integrated Derived PIV Credential solution allows for seamless and rapid deployment of secure PIV credentials to any managed iOS device and gives employees the ability to authenticate to secured enterprise applications using derived PIV credentials from their mobile devices.

The enterprise administrator can leverage the existing Workspace ONE policy management framework to enable derived, credentials-based authentication for their users and also choose which enterprise applications are required to be accessed using derived credentials.

Once a device is enrolled via Workspace ONE, the users can use the Workspace ONE PIV-D app and the Entrust Identity Enterprise Self-Service Module (SSM) to generate the derived credentials on their mobile device. Users authenticate to the SSM using their physical PIV smart cards, which allows them to request their derived mobile credentials post so they can use the Workspace ONE PIV-D app to create and store the credentials in their mobile device.

FIPS 201-2 COMPLIANT DERIVED PIV CREDENTIALS



Learn more about our IAM solutions at Entrust.com

Entrust and VMware integrated derived PIV credential solution

For more detailed information, please call 888.690.2424 or visit **entrust.com** or **workspace.com**.

About VMware

VMware Workspace ONE® is an intelligence-driven digital workspace platform that simply and securely delivers and manages any app on any device by integrating access control, application management, and multi-platform endpoint management. Workspace ONE integrates Unified Endpoint Management™ technology (formerly VMware AirWatch®) with virtual application delivery (VMware Horizon®) on a common identity framework. With Workspace ONE organizations can now evolve siloed cloud and mobile investments, enabling all employees, devices, and things across the organization to accelerate their digital transformation journey with a platform-based approach.

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223