Entrust Datacard™ and VMware® Workspace ONE™ Building Strong Alliances for an Integrated Mobile Identity Assurance Solution

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

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 VMware Workspace ONE to reduce IT cost and complexity
- Flexible deployment: on-premises or fully-managed cloud service

Secure your mobile workforce with a complete, end-to-end NIST SP 800-157 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, doesn't mean that it is, or will provide, a secure, seamless experience.

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

VMware Workspace ONE, powered by AirWatch unified endpoint management technology, and combined with Entrust Datacard certificate-based, mobile smart credential technology, provides secure physical and logical access control 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.

Entrust Datacard™ | vmware®

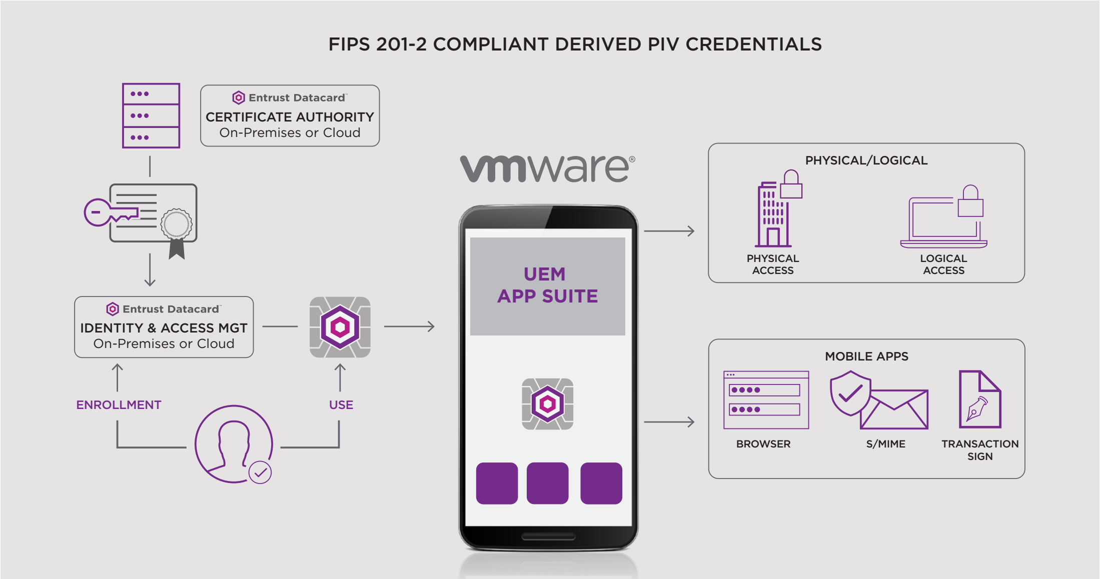
Why use VMware Workspace ONE and Entrust® IdentityGuard?

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 Datacard and VMware Workspace ONE integrated derived PIV credential solution allows for seamless and rapid deployment of secure PIV credentials to any managed iOS or Android device and gives employees the ability to authenticate to secured enterprise applications from their mobile device using derived PIV credentials.

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 must be accessed using derived credentials.

Once a device is enrolled via Workspace ONE, users can use the new VMware PIV-D Manager app and the Entrust IdentityGuard 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 VMware PIV-D Manager app to create and store the credentials on their mobile device.



For more detailed information, please call **888.690.2424** or visit **entrustdatacard.com** or **vmware.com.**

About Entrust Datacard Corporation

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide. For more information, visit **entrustdatacard.com**.

About VMware

VMware software powers the world's complex digital infrastructure. The company's compute, cloud, mobility, networking and security offerings provide a dynamic and efficient digital foundation to over 500,000 customers globally, aided by an ecosystem of 75,000 partners. Headquartered in Palo Alto, California, this year VMware celebrates twenty years of breakthrough innovation benefiting business and society. For more information, please visit **vmware.com.**

Entrust Datacard™

Corporate Headquarters
1187 Park Place
Shakopee, MN 55379 USA

Phone: +1 952 933 1223
info@entrustdatacard.com
entrustdatacard.com