DATA SHEET

Entrust Identity Enterprise and Omnissa Workspace ONE

Secure your mobile workforce with a derived PIV credential solution

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 not only 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. The readers are expensive and their bulky designs clash with the intuitive design of mobile devices.

In other words, just because it's labeled smart doesn't 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 with on-premises or fully managed cloud service

omnissa™

ENTRUST

SECURING A WORLD IN MOTION

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.

Solution

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

Entrust certificate-based, mobile smart credential technology, combined with Omnissa 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

Why use Entrust Identity Enterprise and Omnissa Workspace ONE?

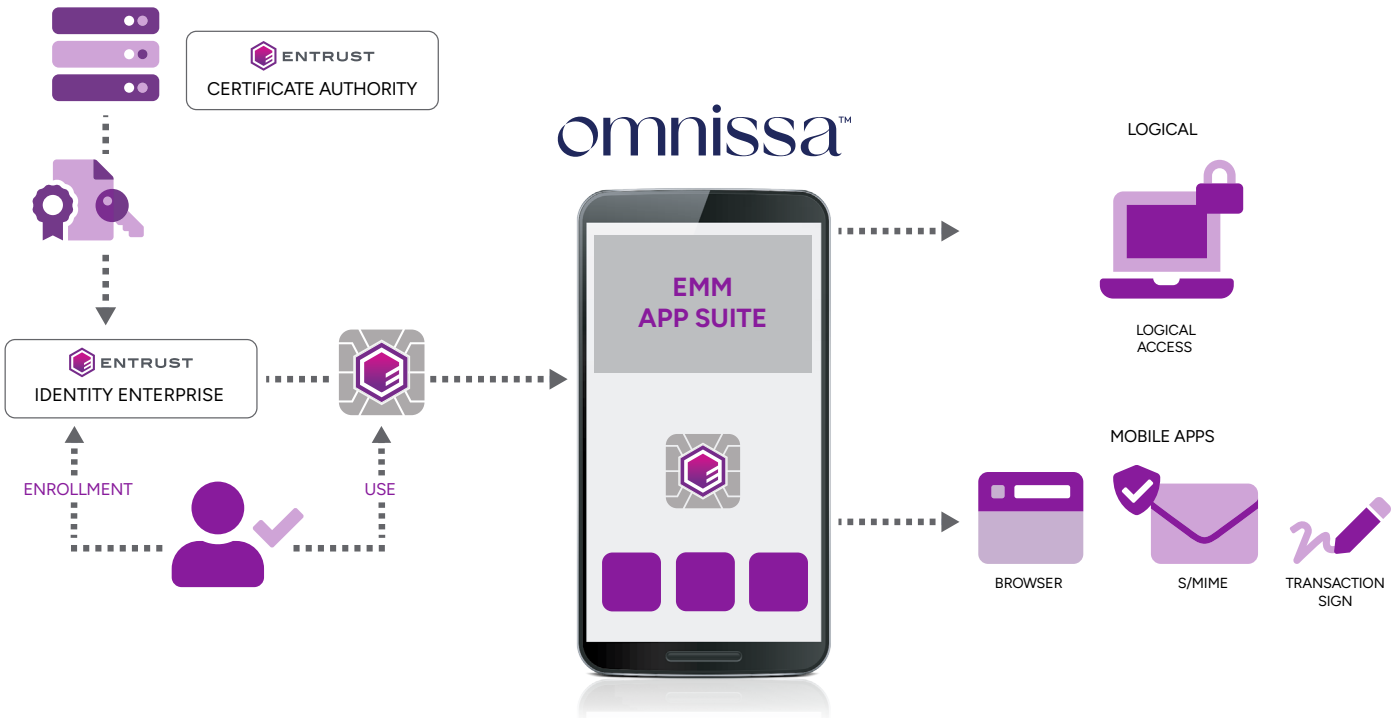
When you provide mobile employees trusted identities to complete secure transactions all through a seamless user experience, you not only maximize valuable resources but you also optimize the usefulness of trusted identities. While federal mandates serve as a catalyst for the use of derived credentials,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

The Entrust and Omnissa 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



About Omnissa

Omnissa is the leading digital work platform company, empowering the world's dynamic workforces to do their best work from anywhere. The company's AI-driven workspace platform helps organizations and their people unlock exponential business value with industry-leading solutions that include Unified Endpoint Management, Virtual Apps and Desktops, Digital Employee Experience and Security & Compliance. Trusted by 26,000 customers worldwide, Omnissa has a 20-year track record in defining digital workspaces. Omnissa, formerly VMware End-User Computing, is a privately-held company with 4,000 employees around the globe. For more information, visit www.omnissa.com.

About Entrust Corporation

Entrust is an innovative leader in identity-centric security solutions, providing an integrated platform of scalable, AI-enabled security offerings.

We enable organizations to safeguard their operations, evolve without compromise, and protect their interactions in an interconnected world – so they can transform their businesses with confidence. Entrust supports customers in 150+ countries and works with a global partner network. We are trusted by the world's most trusted organizations.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION