



ENTRUST



Entrust Derived PIV Credentials

HIGHLIGHTS

Best in class simplicity & security for mobile users

Mobility transforms organizations by providing authorized users with anytime-anywhere access to applications, resources, and information. 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. As more agencies adopt mobile-first models, authenticating access to sensitive data becomes more important than ever.

KEY FEATURES & BENEFITS

- Anytime, anywhere access to applications, resources, and information
- Unified PIV authentication for desktop, mobile, and cloud use cases
- Streamlined implementation and integration
- Greater efficiency and cost effectiveness with faster deployment and enrollment
- Seamlessly adapts to the evolution of mobile OS and MDM/EMM platforms
- Deployment option that fits your existing infrastructure — on-premises or fully managed cloud service
- Increased ROI when you extend your capabilities to mobile



Derived PIV Credentials

HOW IT WORKS

A complete service package

Compliance and security are essential, but managing IT deployments typically includes many challenges. Our Derived PIV Credential professional services help you specifically address those challenges and meet your unique needs.

Simplify your certificate management infrastructure by evaluating an on-premises or hosted PKI service.

Support heterogeneous authentication needs from smart cards to OTP tokens to advanced adaptive solutions, all on one unified platform.

Solves the challenges you face

Gain agility and flexibility to support a variety of use cases, from traditional desktop authentication to secure access to digital applications. This includes:

- Website authentication
- VPN authentication
- Workstation authentication
- Encrypted email
- Digital signatures

End-to-end support

Get dedicated support and expertise for each step of planning, implementing, and managing your Derived PIV Credential solution post-implementation, even as your digital ecosystem evolves.



Log in to workstations with wireless Bluetooth



Authenticate to VPN, web, and SaaS apps



Native authentication to EMM applications



Physical access to doors & kiosks via NFC or QR code



Derived PIV Credentials

Unmatched expertise

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. In alignment with NIST SP 800-157, our Derived Credentials professional services help federal agencies and enterprises leverage mobile devices while remaining compliant with the HSPD12/FIPS 201-2 PIV requirements.

EMM-readiness consultation

Entrust experts help build a Derived PIV Credential solution that can fully and seamlessly integrate with leading Enterprise Mobile Management (EMM) platforms, including Microsoft Intune, MobileIron, and VMware AirWatch. EMM integration provides enhanced protection and policy control, as well as a more transparent user experience – no need for OTPs.



Learn more at
[entrust.com](https://www.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
info@entrust.com [entrust.com/contact](https://www.entrust.com/contact)