

DerivID

A New Era in Secure Mobile User Identity Validation

Derived Credentials for PIV and CAC



DerivID is a patent pending, first-of-its-kind derived credentials solution for PIV and CAC that validates the identity of mobile users seamlessly, simply and securely. It exceeds NIST and DISA security standards and eliminates the need for an external card reader. Our credential issuance process guarantees the highest level of assurance.

The gold standard in mobile user identity validation

DerivID is the ideal solution for validating the identity of mobile users: government employees and contractors who need to access networks and applications or to digitally sign documents and more, in a secure manner.

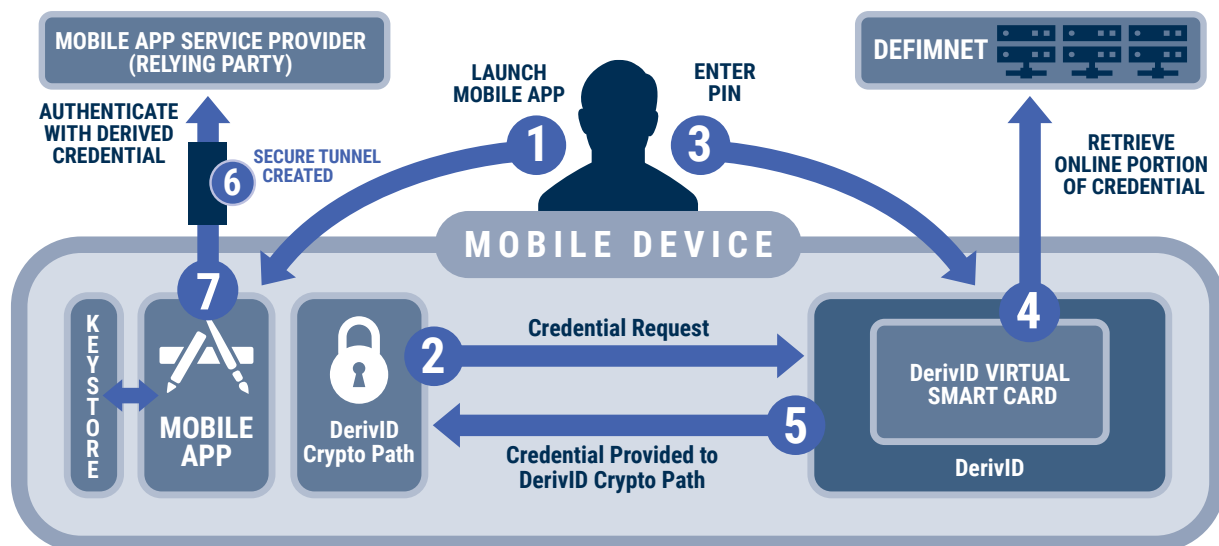
Part of the Route1 suite of patented security solutions, **DerivID** leverages deployed and fully accredited infrastructures (DEFIMNETs) that are available to DOD and civilian government, making **DerivID** seamless and simple to deploy and scale.

Unlike other derived credentials solutions, **DerivID** eliminates vulnerabilities associated with brute force attacks, including dictionary attacks. It also enables the detection and prevention of multiple sign-in attempts.

DerivID is designed to integrate and actively function with multiple Certificate Authorities on the Federal Bridge. It integrates seamlessly with leading MDM and EMM providers and supports the following Apps: native, MDM/EMM, and custom. APIs are available for custom mobile App development.

More than ever before, you need to securely validate the identity of mobile users while reducing risk. **DerivID** is the answer.

How it works



Simple. Secure. Trusted.



Route1's security solutions are trusted by the U.S. Department of Homeland Security, the U.S. Department of Defense, the U.S. Navy, and other government and enterprise organizations.



Secure processes & technology

- Architected based on NIST SP 800-157
- Patent Pending High Security Smart Card technology that eliminates the possibility of brute force attacks – including dictionary attacks
- Configurable user re-authentication triggers and credential validity periods
- Enables the detection and prevention of multiple sign-in attempts

Flexible solution

- Automated credential lifecycle management
- Designed to integrate with existing Certificate Authorities on the Federal Bridge
- Actively functions with multiple Certificate Authorities
- More cost-effective than other derived credentials technologies
- Includes Route1 24/7/365 expert support

Seamless Deployment

- Eliminates the need for an external reader currently required to authenticate with a CAC or PIV card
- Deploys and scales simply and seamlessly
- Integrates with leading MDM and EMM providers
- Accredited infrastructures already deployed and available to both DOD and civilian government
- Level of Assurance 3 (LOA3)

Excellent usability

- Android and iOS-compatible
- Support for both multiple user credentials per mobile device and multiple user devices
- Supports native, MDM/EMM and custom Apps, with APIs available for mobile App development
- Operates in both online and offline mode
- Self-service: no security officer required to facilitate issuance of derived credentials

Try DerivID! The gold standard in mobile user identity validation.

For more information or a free trial, contact your sales representative today.



Route1 protects government and enterprise from the risk of data loss due to unauthorized mobile access and privacy non-compliance, while enabling a more productive workforce.

For more information

+1 866-371-1780

sales@route1.com | www.route1.com