EXECUTIVE BRIEF

HID Derived Credential Solution

The mobile credential in effect is derived from the primary credential ensuring that it can only be provisioned to the right user.

Government Grade High Assurance Security to Manage FIPS 201-2 Compliant PIV Credentials for Mobile Users

PKI-based digital certificates can significantly increase an organization's cybersecurity, by replacing passwords and asserting a trusted identity. For security-sensitive organizations, these digital certificates must be protected.

In today's mobile and cloud-enabled environment it is harder to do that. HID's derived credential solution helps bridge that gap by provisioning digital certificates on mobile devices so that the user can access their IT resources on their mobile device with as high a level of security as they do on their managed workstations and laptop computers. Once it is verified that the user is in control of their primary credential such as a PIV card, the certificates are provisioned to the mobile device.

The mobile credential in effect is derived from the primary credential ensuring that it can only be provisioned to the right user. A typical deployment will provide authentication and digital signature certificates that ascertain the user's trusted identity and provide a way to differentiate the mobile credentials from the primary credentials.

The user will also receive on their mobile device a recovered version of the same encryption certificate that is present on the primary credential – ensuring that users can decrypt data and emails on their mobile device just as well as they can on their computers. Organizations can now be assured that the right person is being authenticated and meet the appropriate assurance level, as defined in NIST SP 800-63.

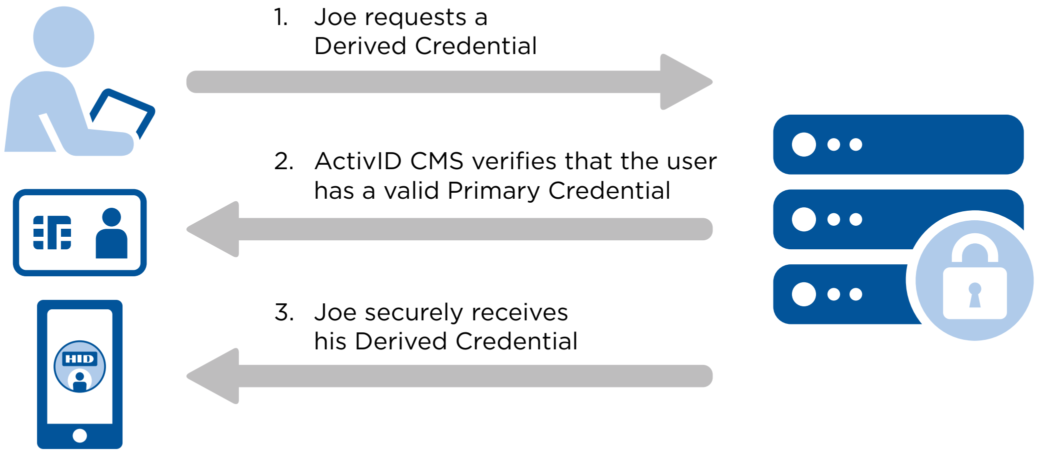
HID's derived credential solution is compliant with NIST FIPS 201-2 and SP 800-157, and checks that the primary credential's certificates are still valid seven days after issuance of the derived credential. Derived credentials that are in violation of security policy can be remotely revoked.

HID's derived credential solution leverages the native capabilities of the user's mobile device, enabling secure access to web sites, secure email and other uses cases using the mobile OS native apps as well as benefiting from the device FIPS 140-2 certification when available.

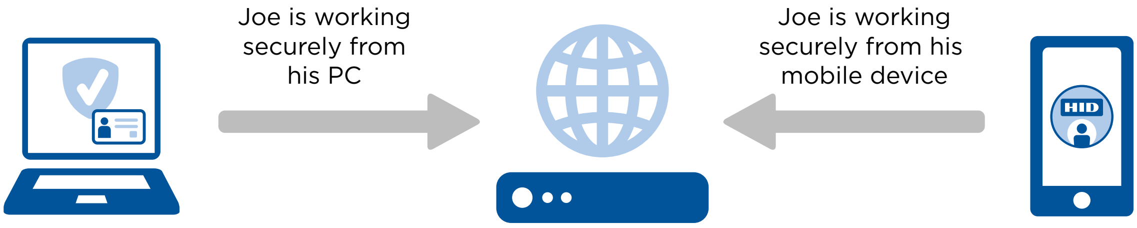
HID's derived credential solution helps ensure organizations that they can do business securely on their mobile devices while remaining compliant with mandates like HSPD-12, and do so with self-service capabilities providing easy and convenient deployment of derived credentials for large organizations.

HID DERIVED CREDENTIAL SOLUTION

HOW IT WORKS

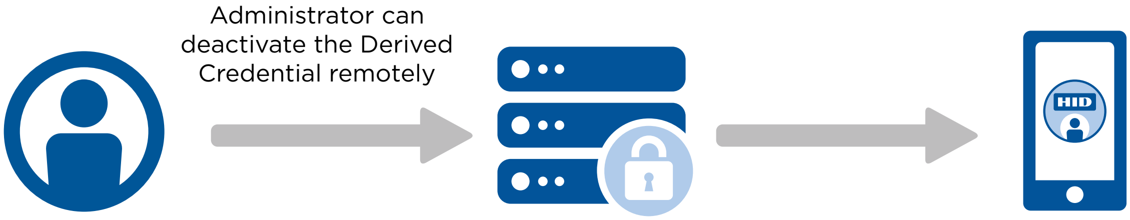


1. Joe requests a Derived Credential
2. ActivID CMS verifies that the user has a valid Primary Credential
3. Joe securely receives his Derived Credential



Joe is working securely from his PC

Joe is working securely from his mobile device



Administrator can deactivate the Derived Credential remotely