DERIVED CREDENTIALS

As today’s IT infrastructures extend beyond traditional boundaries into the Cloud and the number and variety of mobile devices continues to grow, organizations struggle with securing remote access and protecting data. At the same time, employees need to use mobile devices, including laptops, tablets, smartphones, and other computers, to access e-authenticated services, to do work whenever they want, wherever they are located. Automating secure access while accommodating the end user can pay off with increased productivity, and increase security while lowering costs.

Until recently, users required to authenticate with their PIV or CAC card were restricted to working on their laptops and PCs, where a card reader was plugged in and sat on their desktop. But as mobility increased, there were soon available portable, plug-in readers and device cases with built-in readers. Users now had a physical card reader that could be carried with them and used when needed on the mobile device—depending, that is, on whether there was a reader or case that was compatible with their mobile device and Operating System, and integrated with the apps they needed to use.

A better way is now available that eliminates compatibility issues and form factor restrictions; it also eliminates the need for that extra piece of hardware—the reader. Enter the derived credential.

What is a Derived Credential?
Defined in NIST Draft SP 800-157: “…standards-based, secure, reliable, interoperable PKI-based identity credentials that are issued by Federal departments and agencies to individuals who possess and prove control over a valid PIV Card.”

An interoperable or federated credential is critical to secure access to e-authentication applications and services from any location.

Why is a Derived Credential needed?
Draft NISTIR 7981 - Mobile, PIV, and Authentication, states “… leverage both the investment in the PIV infrastructure and the unique security capabilities of mobile devices, such as smart phones and tablets.”

This is accomplished by using the digital certificate on the mobile device to automatically authenticate the user and/or device to gain authorized access to PKI-based network connections, applications, and services without the smart card or smart card reader. The benefits are compelling.

User productivity is the most significant factor when determining the benefits and Total Cost of Ownership (TCO) of deploying a federated derived PIV credential. Eliminating end-user tasks associated with using a traditional smart card for logical access will prove to be the most valuable for the organization.

The elimination of physical card readers has multiple benefits: users have the convenience of true mobility and a seamless mobile work experience. They no longer have to carry extra hardware, and aren’t restricted to devices that support their reader options. With no physical card used, there’s no physical card to remove which can interrupt the secure transactions. Without having to find and purchase new readers for new devices or replace broken readers, cost savings are also realized.

Can Derived Credentials work in my ecosystem?
WidePoint, through its subsidiary Operational Research Consultants Inc. (ORC) designs security solutions using standards-based technologies and COTS products, in order to accommodate the wide variety of mobile devices and security containers available in the market today. Our process will allow issuance of derived PIV credentials via secure cloud services to:

- SD and MicroSD cards
- Trusted Platform Module (TPM)
- SIM cards
Since WidePoint’s ORC has been a trusted partner to the U.S. Federal Government for over 20 years, your organization can be confident that the WidePoint Derived PIV Credential will be fully compliant with the final release of SP 800-157. The staying power of our solutions is based on the foundation built from our operational experience and certifications as an authorized Certificate Authority (CA) for the Department of Defense External Certificate Authority (ECA), GSA Access Certificates for Electronic Services (ACES), Transportation Workers Identification Card (TWIC), Federated Identity Cross Credentialing (FiXs) and the GSA Shared Service Provider (SSP) Program. To complete the authentication process, we provide global Federated Validation Services through our certified Cloud Services for all of these certificates on all devices.

**WidePoint Derived Credential Enrollment Process**

1. **Device Enrollment Request**
The user initiates the process by starting a device enrollment request via the WidePoint Web Enrollment portal.

2. **Mobile Application Installation & Configuration**
The user installs the mobile app on the device and is guided through instructions on the app to complete installation and configuration.

3. **Cryptographic Credential Derivation**
Cryptographic Credential Derivation is the process by which the Certificate Signing Request for the Derived Credential is digitally signed (cryptographically linked) to the primary credential, providing strong non-repudiation in the event of an audit.
4. **Enrollment Process (EST Simple Enroll)**
   The Automated Enrollment Process uses the EST [RFC7030] protocol. WidePoint provides a fully compliant EST RA, backed by a CMP [RFC4210] bridge back to the primary CA.

5. **Certificate Issuance Approval (CA)**
   The customer may configure their CMP endpoint (CA or IDCMS) to require approval before issuing a mobile credential.

6. **Device KeyStore Export**
   Once the App has been issued a credential, it builds a PKCS12 file that includes the key it generated. Installation for the PCKS12 data is mobile platform-dependent.

   For the mobile OS, a KeyChain Install Intent is broadcast which launches the KeyChain Install Activity. This activity prompts the user for their PKCS#12 password (chosen earlier), which they enter into the appropriate dialog box. The credential, including the Certificate Chain, is then available for all other apps on the device.

7. **After Issuance…**
   After issuance, the derived credential can be automatically stored in the directory under the user Certificate X.500 attribute. This allows bidirectional replication to populate the Customer’s primary directory with the new credential. Finally, both the primary and derived credentials are returned to WidePoint Authority.

---
