Understanding derived credentials for the federal government

BY FEDSCOOP STAFF

Derived Credentials offer a NIST-compliant method to protect government data on mobile devices. But lagging agency adoption is constraining workforce productivity, driving employees to seek work-around solutions and leaving CIOs scrambling to offer secure mobility.

NIST defines a derived credential as an alternative token to create strong authentication with mobile devices, such as smart phones and tablets.

Derived credentials offer government agencies a reliable, user-friendly and compliant method for adding strong authentication to mobile devices. This approach also gives agency CIOs a proven alternative to costly and cumbersome physical personal identity verification (PIV) card readers many federal employees are required to use to access government information systems.

So why is the government struggling to adopt derived credentials at a time when agencies are also looking for ways to address the deeper challenges of improving workforce productivity and reducing IT friction — which derived credentials could help to accomplish?

A recent FedScoop study revealed half of government IT users experience moderate-to-high levels of friction using smartphones and tablets to access the information they use for work; and nearly 6 in 10 government IT users say multiple password requirements hinder access to apps and information. Two-thirds of government IT users and half of government IT managers polled ranked single sign-on to all applications on their devices among the top three things that would make their digital experience more productive at work.

Significantly, half of government IT users in the study say if they had tools like virtual digital workspaces to reduce that IT friction, they could gain four or more hours of productivity per week. That equates to more than 200 hours of increased productivity per person per year.

OVERCOMING MISCONCEPTIONS ABOUT DERIVED CREDENTIALS

The federal government faces two main challenges to the adoption of derived credentials: misconceptions around complexity and misunderstanding regarding use and cost.

IT FRICTION

1/2
Experience "moderate-to-high levels of friction" using **smartphones and tablets**

58%
Say multiple password requirements **hinder access** to apps and info

SINGLE SIGN-ON

2 in 3

Government IT users and **HALF** of government IT managers ranked **single sign-on to all applications** on their devices among the **top three** things that would make their **digital experience more productive at work.**

The National Institute of Standards and Technology (NIST) defines a derived credential as an alternative token to create strong authentication with mobile devices, such as smart phones and tablets.

The derived credential is not a new form of technology; instead it is an alternative methodology and process by which an agency first authenticates a user with their existing Personal Identity Verification (PIV) card in order to receive an alternative token that can be used to authenticate that person from their mobile device. This nuance is often misunderstood.

Eugene Liderman, director of product management at VMware, who focuses on security and privacy, says agencies need to better understand and interpret the NIST guidelines around derived credentials and how they fit under strong and overall mobile security. Agencies can leverage this alternative method as part of their overall multi-factor strategy for mobile devices without smart cards and readers, which are clunky and impractical for mobile devices.

"A lot of people think of derived credentials as a silver bullet that's a technological breakthrough that is super complicated," says Liderman. "In fact, it's not a new technology; it's more of a framework, a procedure, a flow of how you enroll and get a derived credential onto your device and use it. It's not so different from what we do today, and there is not as much friction to get going with it."

In many government organizations, smart cards replace the need for a username and password by requiring that an employee physically insert a card into a reader on their computer and then enter a static PIN. By utilizing smart cards, agencies bolster security by requiring employees to authenticate by marrying something they have with something they know.

While smart cards can work relatively easily with desktops and laptops, they don't work well on mobile devices. Liderman says another issue is the misconception that a derived credential is somehow derived from the actual smart card, which is not technically feasible.

Derived credentials are not just a niche solution for the public sector. The private sector could also benefit from derived credentials to protect their workforce and digital assets when using technologies like smartphones, tablets or cloud solutions. By comparison, the government is further behind on the use of cloud solutions, as well as mobile device solutions like tablets, to accomplish day-to-day activities.

MOBILE SECURITY CHALLENGES IN GOVERNMENT

The government operates in an environment often defined by smart cards and has only a general awareness of derived credentials. VMware's Liderman says the myopic focus on smart cards limits government's ability to adopt full mobility in a manner that meets regulations, provides more flexibility for employees and increases productivity, while providing a similar level of security as smart cards.

> **"A lot of people think of derived credentials as a silver bullet...**that is super complicated. In fact, it's more of a framework, a procedure, of how you enroll and get a derived credential onto your device and use it. It's not so different from what we do today, and there is not as much friction to get going with it."
>
> **— Eugene Liderman, Director of Product Management, VMware**

Using smart cards with mobile phones is not a feasible alternative to derived credentials. An external smart card reader incurs a hardware cost, burdens the user with the need to carry another device that connects via USB or Bluetooth to the mobile phone and requires specific applications that can interface with the smart card reader. These applications also incur operational costs and reduce the agency's options regarding which applications they can use.

Using a smart card on a mobile device provides a poor and slow user experience and is confusing to use and troubleshoot. Derived credentials can provide multi-factor authentication with a fast and seamless user experience for government users.

More importantly, using a smart card on a mobile device provides a poor and slow user experience and is confusing to use and troubleshoot. With government users looking for a faster, easier and less frustrating experience, derived credentials can provide multi-factor authentication with a fast and seamless user experience.

In an attempt to mitigate the need to use smart cards with mobility devices in the government, many agencies are simply not enforcing the use of strong authentication on smartphones or mobile devices like tablets.

This approach goes against federal guidelines, specifically around FIPS 201 and HSPD-12. With the creation of NIST Special Publication 800-157, federal agencies now have a viable alternative:

> *"NIST has recently released Special Publication (SP) 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials...to provide the technical details for a system by which mobile devices such as smart phones and tablets are provisioned with PIV credentials, allowing the mobile device to take the place of the smart card for remote authentication to federal systems." — NIST*

Despite providing a foundational direction for agencies to employ mobile security standards, NIST SP 800-157 often lacks details for implementing derived credentials. This can lead agencies to different interpretations of the regulation and how derived credentials produce the required level of security. Varying interpretations also create friction between the teams trying to deploy technology like derived credentials and the teams working to ensure the technology meets compliance standards.

UNDERSTANDING HOW DERIVED CREDENTIALS WORK

The biggest issue most agency officials face is understanding how derived credentials work. Often the technology is misunderstood as a complicated solution that stems from some type of technological breakthrough.

In reality, derived credentials are a framework that creates a process to enroll a user, authenticate that they are who they say they are and allow secure access to applications on a device. In essence, it's not too different from what the government does today with the use of traditional smart cards. Understanding this similarity can make the implementation of derived credentials easier than expected.

A derived credential, as defined by NIST SP 800-157, is an alternative token, which can be implemented and deployed directly with mobile devices, such as smart phones and tablets. This means that a derived credential is a client certificate that's generated on the mobile device, or issued after an end-user has proven their identity by using their existing smart card during an enrollment process.

Understanding this definition frees agencies to use this technology to bolster mobile security in any agency that uses smart cards today, but doesn't want to use them with their mobile devices, such as:

- Department of Defense (DoD)
- Federal Civilian Agencies
- State & Local Agencies
- Federally Funded Research & Development Centers (FFRDC's)
- Federal System Integrators
- Other Regulated Verticals (i.e. Financial & Healthcare)

HOW DERIVED CREDENTIALS WORK:

1. The user enrolls for a derived credential through a self-service portal hosted by the derived credentials provider, using their existing smart card (i.e. CAC or PIV), and either generates a QR code or a one-time password.
2. The user launches the derived credentials application on their mobile device and enters the information from step one.
3. The derived credentials application generates a set of credentials, which can then be used for various applications and profiles on the mobile device.

In fact, the Department of Defense uses a derived credentials program that has netted some impressive results. The DoD-created "Purebred" program is a cryptographic key management server and set of apps for securing mobile devices. It focuses on separating key management from device management, thereby allowing key management to maintain its integration with a separate, public key infrastructure (PKI). The result is consistent mobile security across the DoD enterprise, and device management that can vary with different operational scenarios.

WHAT FEDERAL LEADERS NEED TO KNOW

When appropriately used, derived credentials open up a new, wider world of mobile devices for agencies, where users are no longer tethered to their laptops or desks in a manner that is not compliant. They also provide role-based security, in which the device is just an interface to give a user access to apps and data they need to work.

Derived credentials also empower managers with control over applications and data, even when they don't own or have control of the device. Finally, with derived credentials, users have the flexibility to access the apps and data they need for work, anytime, anyplace, from any device.

Before approaching derived credentials, agency leaders need to understand how much of their enterprise they want derived credentials to manage. In many ways, it's about understanding your level of comfort with this technology, including determining if your agency should learn to "walk" before it "runs" into full immersion.

Asking and answering some questions can help you determine the best approach:

1. **Which types of devices do you want to implement derived credentials on?** Desktops already have smart cards, so they may be a lower priority. Also determine what percentage of iOS vs Android devices your agency operates.
2. **Do you require that your derived credentials be chained off the Federal Bridge or not?** The Federal Bridge, operated by the General Services Administration (GSA), provides cross-certification among trust domain PKIs. Using the Federal Bridge implies that the derived credentials solution must be tied to this service, which can add complexity to the implementation. Your agency may have some immediate use cases it can achieve without issuing derived credentials that are chained from the federal bridge (i.e. authenticating to email) and thereby learn to walk first.
3. **Which levels of identity assurance do you want to meet?** Understand Levels of Assurance (LOA) and determine the reasons you may want higher levels of assurance, such as LOA 3 versus 4. LOA describes four identity authentication assurance levels for e-government transactions, which include:
   - Level of Assurance (LOA) 1: Little or no confidence in the asserted identity's validity.
   - Level of Assurance (LOA) 2: Some confidence in the asserted identity's validity.
   - Level of Assurance (LOA) 3: High confidence in the asserted identity's validity.
   - Level of Assurance (LOA) 4: Very high confidence in the asserted identity's validity.

   LOA 4 can add complexity because it requires an in-person enrollment and use of biometrics. This addition can needlessly complicate a derived credential implementation. Agencies often try to set the bar too high and shoot for LOA4. It's important to note that the perceived requirement to use LOA4 does not stem from the NIST SP 800-157 standard, although it's mentioned in the standard. It isn't needed to be compliant, but rather is a definition of what level of privilege that credential provides.
4. **Do you have the correct combination of software and licenses?** With derived credentials, there are no hardware costs and no additional fees as long as agencies have the correct license bundle. If agencies want to use a third-party solution, there's a cost per user or credential, but it's often less than the cost of hardware.
5. **Do you plan to integrate derived credentials in to your overall Identity & Access Management (IAM) strategy?** The combination of derived credentials and modern IAM tools is a powerful duo. With this combination, as agencies move to the cloud or further adopt mobile technology, the agency can take advantage of commercially available applications without having to rebuild any of those applications, and while leveraging derived credentials to remain safely authenticated.

PUTTING IT TOGETHER

When moving to derived credentials, agencies should start with a limited scope. Examples could be: access to email and intranet websites or Wi-Fi and VPN. As agencies start getting more comfortable, they can look at deploying derived credentials in conjunction with an identity and access management solution for commercially off the shelf (COTS) apps and various cloud back-ends.

After this evolution in the use of derived credentials, agencies can then start thinking of other lines of business applications where they may want to use this authentication capability, like a catalog or field survey application, for example. At this stage, the mobility and productivity of the agency will reach new heights in a safe and secure manner.

Finally, partnering with vendors that can guide the agency in implementing and using a derived credentials solution that scales is a key step. VMware, for example, can help agencies identify the 56 percent of applications that are not optimized for mobile devices and guide them around that issue.

For more on VMware solutions in the federal market go to www.vmware.com/go/federal.

Download the full Government Workforce Productivity Report.

This article was produced by fedscoop for, and sponsored by, vmware