# February 2015 Federal Mobile Computing Summit Collaboration Session Summary

Tom Suder ATARC

Mike Peck, Gaurav Seth, Mark Russell, Patrick Benito, Marie Collins The MITRE Corporation

Approved for Public Release; Distribution Unlimited. Case Number 15-1362
The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author

## **Executive Summary**

The Federal Mobile Computing Summit took place on February 18<sup>th</sup>, 2015. The Summit included a set of MITRE-Advanced Technology Academic Research Center (ATARC) led Collaboration Sessions that afforded industry, Government, academic, and federally funded research and development center (FFRDC) representatives an opportunity to collaborate, and discuss prominent challenge areas in mobility. In some cases, potential solutions were identified for key challenge areas. The discussions were Government focused with the objective of refining gaps, and identifying features of potential solutions or frameworks.

The Collaboration Sessions covered three key mobility topics:

- Identity and Access Management: Deploying Derived Credentials at the Enterprise Level
- Making Bring Your Own Device a Reality in the Federal Government
- Building Commercial Solutions for Classified Use

This white paper summarizes the results of the Collaboration Sessions and provides detailed actionable recommendations for Government and academia, which are summarized in the table below.

Develop a Government wide reference architecture to provide agencies more guidance on how to deploy derived credentials.

• The reference architecture should address different deployment models that cover the agency owned and managed devices, and Bring Your Own Device (BYOD) use cases.

Create a BYOD group within the Federal CIO Council ISIMC Mobile Technology Tiger Team to address key challenges.

• Key challenges and guidance include: BYOD policy, understadning true cost/benefit of BYOD for the governnt., and help estabilsh an approved product list fo a BYOD program.

Develop a business model that incentivizes more companies to build components for the Commercial Solutions for Classified Program.

• The business model should include incentives to attract both large and small comapanies, and be accompanied with specific information on how to start doing bsiness under the CSfC program.

Create a community built around Government, industry, and academic collaboration to leverage potentially previously untapped academic resources to help advance Government mobility.

• Leverage graduate and undergraduate level research to help solve critical mobility challenges, while attracting students to public service and preparing them for a future career.

# **Table of Contents**

1	Introd	luction	4
2	Collab	oration Session Overview	4
3	Feder	al Mobile Computing Summit Collaboration Sessions	5
	3.1 Ide	entity and Access Management: Deploying Derived Credentials at the	
		ise Level Session	5
	3.1.1	Session Goals	5
	3.1.2	Session Summary	5
	3.1.3	Recommendations	7
		aking Bring Your Own Device a Reality in the Federal Government	
	3.2.1	Session Goals	7
	3.2.2	Session Summary	7
	3.2.3	Recommendations	8
	3.3 Bu	ilding Commercial Solutions for Classified Use	8
	3.3.1		9
	3.3.2		9
	3.3.3	Recommendations	10
4	Summ	ary & Recommendations	10

### 1 Introduction

The Federal Mobile Computing Summit took place on February 18<sup>th</sup>, 2015 in Washington, D.C. The Summit included a set of MITRE-Advanced Technology Academic Research Center (ATARC) led Collaboration Sessions that afforded industry, Government, academic, and federally funded research and development center (FFRDC) representatives an opportunity to collaborate, discuss the main challenge areas in mobility, and discussed prominent challenge areas in mobility. In some cases, potential solutions were identified for key challenge areas. The discussions were Government focused with the objective of refining gaps, and identifying features of potential solutions or frameworks. The discussions were Government focused and at a high-level, not addressing any specific solution and only identifying features of potential solutions or frameworks.

As part of the Collaboration Sessions, MITRE and ATARC invited academia to participate in each of the four challenge areas, and asked participating academics to identify courses of action to be taken to enable improved Government and industry collaboration with academic institutions.

This white paper summarizes the results of the Collaboration Sessions and identifies suggestions and recommendations for Government and academia while identifying crosscutting issues that tie between the different challenge areas.

### 2 Collaboration Session Overview

MITRE and ATARC created an outreach and collaboration process to crowd-source the development of recommendations to key Government challenges. This process focuses on soliciting input from a diverse group of participants and exploits their diverse backgrounds, points of view, and skillsets to create new, novel, and innovative recommendations to key problems.

Each MITRE-ATARC Collaboration Session was a focused and moderated discussion between Government, industry, and academic representatives centered on key mobile challenge areas that were solicited from the Government prior to the event.

The challenge areas are as follows:

- Identity and Access Management: Deploying Derived Credentials at the Enterprise Level
- Making Bring Your Own Device a Reality in the Federal Government
- Building Commercial Solutions for Classified Use

Participants discussed current problems, gaps in current and planned work programs, potential solutions, and ways forward for each of the challenge areas. Section 3 outlines the goals, outcomes and summary of each of the three collaboration sessions.

# 3 Federal Mobile Computing Summit Collaboration Sessions

The outcomes of the four Collaboration Sessions are included in this section. This section elaborates on the Session goals, a summary of the discussions, and identification of relevant outcomes.

# 3.1 Identity and Access Management: Deploying Derived Credentials at the Enterprise Level Session

This session featured a discussion on Derived Personal Identity Verification (PIV) Credentials, an emerging technology standard that aims to provide strong, HSPD-12 compliant authentication on mobile devices. With the newly published NIST standard (SP 800-57) and vendor solutions beginning to appear, some key questions about how to implement, manage, and integrate these solutions remain. The session sought to elicit Government's expectations for Derived PIV Credentials and industry's views on what is technically possible, and highlight some areas in need of further consideration.

#### 3.1.1 Session Goals

- Identify any agencies and organizations that are currently deploying Derived PIV Credentials
- Identify lessons learned from early adopters
- Identify gaps in policy and technical guidance hindering agencies from fully adoption Derived PIV Credentials
- Discuss what the next generation of Identity and Access Management (IdAM) will look like

#### 3.1.2 Session Summary

The session began with a "Derived PIV Credentials 101" presentation summarizing the contents of NIST SP 800-157. Briefly, Derived PIV Credentials are PKI credentials issued to mobile devices to users who already have PIV credentials. Strong identity proofing and background checking are performed prior to issuing a PIV credential. When enrolling for a Derived PIV Credential, the user proves possession of a valid PIV card, eliminating the need for further identity proofing and linking the new credential to the user's well-established HSPD-12 identity. NIST SP 800-157 provides requirements and guidance for how agencies can issue, manage, and use Derived PIV Credentials.

The audience members were asked to identify use cases for Derived PIV Credentials. The most obvious use case is user authentication to enterprise services on government-issued devices, but a wide range of use cases were discussed. Among the more challenging use cases were issuing credentials to unmanaged or partially managed devices (e.g., BYOD, Corporately Owned Personally Enabled, or devices belonging to partner agencies). There was some interest in enabling users to use their agency credentials to authenticate to other agencies' resources, a capability that remains somewhat challenging with PIV cards. Multiple participants brought

up multi-user devices such as those used in flight screening by TSA agents, and how credentials would be issued and managed on them. Finally, there was interest in using Derived PIV Credentials as a substitute for the PIV card for unlocking workstations or for physical access control using NFC or other wireless technologies. These uses are currently out of scope per NIST SP 800-157.

The process of issuing and provisioning Derived PIV Credentials was then discussed, with the pros and cons of key storage in hardware secure elements, the OS native keystore, and third-party keystore provider apps. Most approaches are currently hampered by the lack of native mobile OS interfaces for third-party PKI library integration. This combined with app sandboxing requires the integration of vendor-specific SDKs with each mobile app that will use the credential. Credential issuance poses further challenges in ensuring that a chain of trust is maintained between the user's PIV authenticated registration session and the issuance of credentials to the device. Likewise, there is typically a need to authenticate the device and ensure it is under agency management and control, except in the BYOD or partner device use cases mentioned above. Questions remain about implementation specifics, including how much of a role MDM can play. Most of the audience would prefer an unattended, over-the-air remote issuance capability, though some would find an inperson "kiosk" solution acceptable.

In the subsequent discussion on operational use of the credentials, user experience concerns were expressed regarding the need to enter a separate PIN for Derived PIV authentication. In some cases this would be a third authenticator, in addition to a device unlock PIN and a "secure container" password. Participants had practical questions about providing support, including the need to unlock credentials following excessive failed PIN attempts. With users having multiple devices, some might have several credentials, causing potential confusion when the user calls in for assistance with a credential on a particular device. The group was agreed that users would need to be able to authenticate to all the mobile apps on a device with a single credential, and that issuing multiple credentials (such as one for each app) would prove unmanageable.

Finally, the group discussed credential management and governance issues, including the business processes for managing credentials. On the subject of a manual approval process for users to obtain credentials, the group was agreed that the ideal solution would be for users to be automatically pre-approved when they were issued mobile devices. Questions were raised about potential impacts on PKI licensing, with each user receiving potentially multiple new PKI certificates; agencies will need to discuss licensing options with PKI vendors before pursuing widespread deployment. Managing certificate renewals in anticipation of credential expirations is another key business process that needs to be thoroughly developed in order to avoid costly downtime and user aggravation.

#### 3.1.3 Recommendations

- Agencies need further guidance on practical Derived PIV Credential implementation details such as how to leverage Mobile Device Management (MDM), Credential Management Systems, and other components in derived credential issuance and management. The development of a reference architecture would be helpful, especially if it can address different deployment models (agency-managed devices, BYOD, etc.).
- The lack of standard cryptographic interfaces in mobile operating systems
  makes integration of solutions difficult. Interoperability of multiple vendor
  solutions typically requires one-off, custom integration, which is costly and
  time-consuming. Mobile OS vendors could greatly facilitate integration by
  providing standard cryptographic interfaces that could be used by thirdparty developers.

#### 3.2 Making Bring Your Own Device a Reality in the Federal Government

This session focused on policy and technology challenges and solutions for implementing Bring Your Own Device (BYOD) in the federal government.

#### 3.2.1 Session Goals

- Identify policy advancements that are being made and additional advancements that need to be made
- Identify ideal architectures for BYOD
- Identify where technology needs to advance to make BYOD more usable and more secure

#### 3.2.2 Session Summary

This session began with discussions on policy implications of BYOD. The group agreed that federal agencies implementing a Bring Your Own Device program should provide employees with clear policy guidance. This policy guidance should make clear personal privacy and usability considerations associated with using the agency's BYOD solution, such as any management controls and monitoring that are imposed upon the employee's device. For example, some solutions provide agencies with the technical ability to wipe all data stored on the device or the ability to monitor all installed applications. The group also agreed that agencies should keep these controls and monitoring to the minimum necessary to safeguard enterprise information and should provide assurances to employees of how their personal privacy will be protected, as otherwise employees may be discouraged from participating. The policy should also address situations such as classified data spillage and how the agency will respond.

The discussion shifted towards cost. BYOD has often been touted as a cost saver for organizations. The group agreed that agencies should conduct a cost-benefit analysis before implementing a Bring Your Own Device program. The reason being

is that BYOD may intuitively appear to save money, but there are still costs involved that must be carefully analyzed. The group listed many costs BYOD may include. This list includes software licenses for enterprise services, employee reimbursements for portions of device and service plan costs, and technical support costs. Agencies should compare the cost of implementing a BYOD program with the cost of using government furnished devices obtained through vehicles such as the GSA contract. Regardless of whether BYOD saves money (results may vary based on each agency's use cases and other unique circumstances), the group agreed BYOD may provide other benefits to agencies and employees such as allowing the use of the latest technologies and allowing employees to use a single mobile device for both personal and work purposes rather than have to carry multiple mobile devices. If participation is voluntary, the agency should consider what incentives are provided to employees to participate, and what expenses the agency will incur if employees do not participate (e.g. may need to provide government furnished equipment). A key point on reimbursement was discussed. Specifically, agencies must also determine whether to reimburse employees for using personal devices, and if so how to calculate the reimbursement rate, such as a constant amount per month or a split billing solution that precisely measures enterprise data and voice usage.

The group went on to discuss if agencies should allow all devices to be used, or only devices chosen from an approved list. There is a vast difference in security posture between different types of mobile devices, particularly in whether critical updates to patch discovered vulnerabilities will be provided in a timely manner if at all. The ability of BYOD solutions to properly protect enterprise data is generally dependent on the integrity of the underlying mobile device, so using devices that are susceptible to well-known vulnerabilities can introduce significant risks.

#### 3.2.3 Recommendations

- Provide employees with clear BYOD policy guidance. This policy guidance should make clear personal privacy and usability considerations associated with using the agency's BYOD solution, such as any management controls and monitoring that are imposed upon the employee's device.
- Conduct a cost benefit analysis before starting a BYOD program. Understand the reason behind adopting BYOD, and recognize cost may not be the primary driver.
- Create and maintain an approved product list for BYOD. This will give the employee some freedom for device selection, while still providing the security required.

#### 3.3 Building Commercial Solutions for Classified Use

This session focused on establishing some common understanding between vendors/industry and the Government on the scope and benefits of Commercial

Solutions for Classified (CSfC) and discuss key challenge areas. Prior to the sessions, the leads developed a set of questionnaire to captured feedback from the participants to assist with facilitating an open collaboration.

#### 3.3.1 Session Goals

- Discuss CSfC overall process and key roles
- Discuss factors which will incentivize commercial companies to build commercial solutions for classified use
- Discuss factors which will prohibit commercial companies to build commercial solutions for classified use

#### 3.3.2 Session Summary

The CSfC Collaboration Session started with the discussion on defining CSfC process. Government provided a presentation, which was delivered by Mr. Gaurav Seth (MITRE) to highlight the CSfC overview. Difference between a CSfC component vs. a CSfC solution was debated. In particular, there was some dialogue on how a list of components that have been certified does not automatically equate to a full solution that can be implemented. The question was raised to whether the government should require only CSfC approved integrators to build and implement classified mobile solutions using CSfC components. Initially, it was agreed that, yes, this is the desirable scenario. It was also mentioned for non-mobile projects, this is how things are typically done. At the current time, there are a lack of system integrators with experience building mobile classified solutions. The group conversed about how to get a component product approved for use. Some members commented it was too complex while others still believed mobile products had to go through JITC testing as well as NIAP validation.

Some members represented small businesses trying to get into the CSfC space. They mentioned that the process was difficult to follow for a new business trying to get a product certified. In many cases, to be evaluated against government processes such as CSfC, a vendor requires a sponsorship. Some members felt the process as is was weighted toward established, big players in the industry who had experience navigating government regulations and process. It was mentioned that more guidance on how to take a product completely through CSfC would be very beneficial.

A concern was raised on how a company can spend significant money and resources going through the NIAP and CSfC process and that there was risk of losing their incentive to actually go through the process if individual DAAs continue to allow non-certified products to get deployed. It was expressed that on one hand, the government was trying to come up with a cross organizational standard via NIAP and CSfC but on the other hand, couldn't get individual organizations to agree to the process. It was further discussed that if this continued, it would be a discouragement for manufacturers and solutions providers to go through the NIAP

process if they thought they could circumvent the process by going to the organization directly and demonstrating their product.

There seemed to be a perceived loophole in this process given that a vendor would be granted conditional approval based upon their entry into CSfC process with the thought that they had a certain amount of time to complete the process. But if they failed to complete successfully, it was not clear how that conditional approval would be revoked. It was stated that ultimately it was up to the DAA to approve or not approve a solution for deployment and that it was incumbent upon them to do due diligence to ensure the vendor components successfully completed the CSfC process.

#### 3.3.3 Recommendations

- Create a business model that incentivizes both small, and large, commercial players to participate in CSfC
- Provide more detailed CSfC and NIAP process details with key milestones to help new vendors and other interested partners

# 4 Summary & Recommendations

Several key recommendations emerged as a result of the three Collaboration Sessions. Firstly, many agencies are interested in pursuing a BYOD program. Many agencies see this as inevitable, and part of the next steps of Government mobility. The Government would benefit from have the Federal CIO Council ISIMC Mobile Technology Tiger Team Create a BYOD group within the Federal CIO Council ISIMC Mobile Technology Tiger Team to address key challenges and provide guidance for: BYOD policy, understanding true cost/benefit of BYOD for the government, and help establish an approved product list for a BYOD program.

Secondly, as more agencies look to adopt classified mobility, it will become even more important to help commercial vendors through the process. It is highly recommended that the Federal Government begin to develop a business model that incentivizes more companies to build components via the CSfC process, as well as providing more detailed guidance for new vendors on how to participate in this program.

Thirdly, development of a Government wide reference architecture will be helpful to provide agencies more guidance on how to deploy derived credentials. This will be especially true if it can address different deployment models that cover the agency owned and managed devices, and BYOD use cases.

Fourthly and lastly, create a community built around Government and industry collaboration with academia to leverage potentially previously untapped academic resources. The proposed community will enable communications between the different participating communities. The outcomes of this community include:

- Academia produces higher quality, better-prepared, and "industry-ready" graduates for hire
- Government leverages graduate and undergraduate level research to help solve critical mobility challenges
- Government organizations have an integrated research and advisory capability made up of commercial companies, academic institutions, and federally funded research and development centers (FFRDC)