Draft NISTIR 7981

Mobile, PIV, and Authentication

Hildegard Ferraiolo
Andrew Regenscheid
William Burr
David Cooper
Salvatore Francomacaro

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NISTIR 7981

Mobile, PIV, and Authentication

Hildegard Ferraiolo
Andrew Regenscheid
David Cooper
Salvatore Francomacaro
Computer Security Division
Information Technology Laboratory, NIST

William Burr
Dakota Consulting, Inc.

March 2014

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Interagency Report 7981
14 pages (March 2014)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Public comment period: *March 7, 2014* through *April 21, 2014*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: piv_comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Abstract

The purpose of this document is to analyze various current and near-term options for remote electronic authentication from mobile devices that leverage both the investment in the PIV infrastructure and the unique security capabilities of mobile devices, such as smart phones and tablets.

Keywords

electronic authentication; Derived PIV Credential; PIV Card; microSD; USB; UICC; mobile device; smart phone; tablet

Table of Contents

1. Introduction

In the past decade, mobile devices have already significantly changed business capabilities, allowing employees access to information resources wherever and whenever they need it. These devices are both an opportunity and a challenge. Their unique capabilities – including their always-on, always-connected nature – can facilitate more efficient and effective government, but also create new challenges to ensure the confidentiality, integrity and availability of information accessed by these devices.

This document focuses on the challenge of electronic authentication from mobile devices, defined as the process of establishing confidence in user identities electronically presented to an information system from a mobile device. The Federal government's current approach to electronic authentication in traditional computing devices requires the use of Personal Identity Verification (PIV) Cards, which are "credit card size" smart cards using credentials based in public key cryptography. Users must insert these cards into readers built into, or attached to, the computers they use to access government information. While this approach to electronic authentication works reasonably well with desktop and laptop computers, the same approach for mobile devices, lacking the space for integrated smart card readers, would require bulky add-on readers.

The purpose of this document is to analyze various current and near-term options for electronic authentication that leverage both the investment in the PIV infrastructure and the unique security capabilities of mobile devices, such as smart phones and tablets. While any of the options discussed in this paper could support government security and interoperability requirements, we believe current trends in the mobile device ecosystem argue for a flexible electronic authentication policy that allows for close integration between the credential and the mobile device.

2. Background

2.1 Mobile Devices and Technologies

In recent years, a new class of commercial computer products, "mobile devices," has dramatically disrupted the IT industry while providing many opportunities for better information services and business processes. Mobile devices, such as smart phones and tablets, are powerful, Internet-connected computers, small and light enough to be carried nearly anywhere.

Mobile devices, in the form of mobile phones and Personal Digital Assistants (PDAs), have been available in some form for over twenty years, but advances in technologies and services over the past six years have greatly increased their capabilities and use in the public and private sector. The development of powerful, energy-efficient processors and small, reliable touch screens, along with the now-ubiquitous availability of WiFi and 3G/4G mobile broadband networks, have spurred constant innovation in this space.

Along with the significant capabilities of mobile devices, market pressure is driving the manufacturing of smaller, lighter devices with adequate battery life, at low cost. These constraints drive mobile device manufacturers to limit external ports and distinct computer chips, and focus on integrating features into the System on Chip (SoC) that is the core component of every mobile device.

The unique set of security features and constraints of mobile devices, combined with the different way in which we use and secure mobile devices relative to traditional desktop and laptop computers necessitates the identification and standardization of alternative electronic

authentication mechanisms that leverage the same identity management infrastructure that has already been deployed.

2.2 Personal Identity Verification (PIV) Infrastructure

The deployment of PIV Cards and their supporting infrastructure was initiated by Homeland Security Presidential Directive-12 (HSPD-12), which mandated a common identification standard to enhance security, promote interoperability and increase Government efficiency. HSDP-12 was intended to address wide variations in the quality and security of authentication mechanisms used across federal agencies. It directed the federal government to establish and adopt an interoperable standard providing graduated levels of security to provide agencies with the flexibility to deploy appropriate mechanisms based on their environment and the sensitivity of their data. To meet the goals outlined in HSPD-12, the PIV Card was designed to be interoperable across the federal government – both for physical access to government facilities and logical access to Federal information systems. The PIV Card contains several identity credentials supported by a public key infrastructure (PKI) to provide strong identity assurance in an interoperable manner. To provide a high level of trust in the credentials across the Federal enterprise, the PIV standard established common processes for identity proofing and credential issuance.

Today, federal agencies have issued PIV Cards to the vast majority of federal employees and contractors and the emphasis has shifted from PIV Card issuance to its use for logical and physical access. Applications such as MyPay, Employee Express, and the OMB Max Portal are just a few examples where the PIV Card is used for government network access.

3. Electronic Authentication Approach

With a worldwide market for mobile device sales of approximately 1 billion devices annually, the public sector has limited market pressure to impact security capabilities and features. Instead, features and capabilities are largely determined by consumers purchasing mobile devices for personal use. Despite this challenge, government security needs are generally similar to business needs and consumer applications, including mobile payments and digital rights management. This presents an excellent opportunity for the federal government to continue to work with industry to identify the security practices, standards and guidelines that can support both public and private sector needs.

The mobile ecosystem is highly competitive, with different mobile device manufacturers, platforms, and wireless carriers rapidly implementing and deploying new capabilities, often with different focuses. Allowing for varied implementations and the level of innovation we have come to expect from the mobile ecosystem argues for a flexible approach to electronic authentication from mobile devices to ensure departments and agencies can take advantage of these capabilities.

This section will describe and analyze a number of proposed approaches that leverage the existing PIV infrastructure to authenticate users. Some options are supported by currently available technologies, and others require the development or commercialization of technologies that are not currently available. However, even options supported by current technologies may not be immediately deployable, as additional standardization, testing, or software development may be needed to make these options compatible with government systems as intended by HSPD-12.

These proposals provide a range of options, some perhaps only transitional, facilitating different operational scenarios for mobile devices, from high security government-owned mobile devices, to dual-use bring-your-own-device (BYOD) scenarios.

3.1 Using PIV Cards

One general approach to electronic authentication from mobile devices is to find ways to use the PIV Card itself with the mobile device. Unlike some laptops, mobile devices are generally too small to integrate smart card readers into the device itself, requiring alternative approaches for communicating between the PIV Card and the mobile device.

Currently, using PIV Cards with mobile devices would require the use of third-party smart card readers separate from, but attached to, the mobile device itself. Any time the user attempts to access an IT resource, he or she would need to insert the PIV Card into the separate reader and enter his or her PIN. While this approach is rather cumbersome for users, it has the advantage that agencies would not need to issue and manage another set of PKI credentials for users.

3.1.1 Current Technology Supported Approaches

USB/Bluetooth Card Readers

Description: PIV Cards could be used with existing and new mobile devices with the use of add-on smart card readers. These readers would interface with the mobile device over a wired (e.g., USB, Apple's Lightning) or wireless (Bluetooth) interface. Applications (e.g., browsers, e-mail clients) would need to interface with the smart card reader.
Availability: High – Third-party card readers using Bluetooth, USB, or other proprietary connectors are available for most mobile device platforms. Application support for using PIV Cards through these readers is more limited, which could complicate use.
Benefits: This approach allows the use of existing credentials on PIV Cards, removing the need to provision and manage new credentials to users and devices.
Considerations: This is a cumbersome approach, requiring users to carry their PIV Cards and card readers with them whenever they need to use their devices. This would decrease the portability of these devices and hinder the usability, requiring users to insert their PIV Cards into the devices to authenticate to an information system. Also, while use of wireless Bluetooth readers would slightly mitigate some of the usability concerns, it would do so at the detriment of battery life. In addition, while these readers are commercially available, they are fairly niche devices, and as such, are relatively expensive.

3.1.2 Possible Near-Term Approaches

Near Field Communication (NFC)

Description: Near Field Communication (NFC) uses radio frequency to establish communication between NFC-enabled devices. An NFC-enabled mobile device could interact with a PIV Card and its keys over its contactless antenna at very close range, allowing the mobile device to use the PIV keys without a physical connection. The user would need to hold or place the card next to the mobile the device as she or she enters the PIN protecting the keys on the PIV Card.
Availability: Limited – Many mobile devices on the market do not include NFC. Of those that do, platforms do not necessarily provide the capabilities needed to interact with a PIV Card.
Benefits: Assuming NFC is built into a device, this approach allows the use of the PIV Card without a relatively bulky internal or external card reader.
Considerations: Current PIV Cards greatly restrict the keys that are accessible via the contactless interface, as these cards do not support the establishment of a secure channel between the card and an NFC reader. Revisions to the PIV standards under development at

NIST will include a secure channel specification, enabling the use of these keys over the contactless interface when both the card and reader support the secure channel.

3.2 Using Derived PIV Credentials

As specified in SP 800-63, derived credentials are designed to leverage identity proofing and vetting processes of a user's primary credential. Identity proofing and vetting processes do not have to be repeated to issue a derived credential. Instead, the user proves possession of a valid primary credential as the basis to receive a derived credential. The new derived credentials do not need to be the same type or in the same token as the primary credential.

For the purpose of PIV, possession of a valid PIV Card is the basis to issue Derived PIV Credentials for mobile devices. To achieve interoperability with the PIV infrastructure and its applications, the Derived PIV Credentials are PKI-credentials. The form factor, however, is different than the PIV Card's smart-card form factor by design. While PIV Cards are functionally compatible with mobile devices, they are mechanically incompatible for one reason: the credit card sized PIV Card's packaging is much too big. To address these limitations, Derived PIV Credentials can be issued in form factors that are easier to use with mobile devices. In particular, the approaches proposed below embed or integrate them in mobile devices. They could be remotely provisioned (at a lower assurance level) to users who successfully authenticate with their PIV Cards (possibly using the card on some other device). These approaches can greatly improve the usability of the electronic authentication mechanisms.

The technical details of Derived PIV Credentials are specified in Draft SP 800-157 [SP800-157]. The goal of the Derived PIV Credential is to allow for PIV-enabled e-authentication services from mobile devices to remote systems. Draft SP 800-157 offers several technical solutions in order to accommodate a variety of mobile devices in the market today.

3.2.1 Current Technology Supported Approaches

Software Tokens

Description: Rather than using specialized hardware to store and use PIV keys, this approach stores the keys in flash memory on the mobile device protected by a PIN or password. Authentication operations are done in software provided by the application accessing the IT system, or the mobile OS.
Availability: High – all major mobile platforms provide interfaces for storing and using software-based certificates. However, additional security and interoperability testing may need to be done to ensure suitability for government use, as intended by HSPD-12
Benefits: This approach could be used on any mobile device and does not require specialized hardware.
Considerations: Protecting and using the Derived PIV Credential's corresponding private key using software-based mechanisms potentially increases the risk that the key could be stolen. This approach may provide a lower level of assurance of identity than other methods describe in this document.

MicroSD Tokens

Description: Specialized microSD cards (or similar expansion cards) exist that contain a hardware cryptographic module capable of storing and using a private key. To the mobile device, the microSD with such a cryptographic module would function similarly to a smart card.
Availability: Moderate – Not all mobile devices include microSD slots. While microSD smart card tokens are commercially available, additional security and interoperability

testing may need to be done to ensure suitability for government use, as intended by HSPD-12. Furthermore, mobile OS and application software support is very limited at this time.

Benefits: These cards could be deployed on devices after purchase to add security features. They would provide better protection of the private keys corresponding to Derived PIV Credentials than a software only approach. The token can be ported to other devices supporting microSD tokens.

Considerations: MicroSD cards can be cumbersome to remove from mobile devices. In normal operation, they would remain in the device at all times, but the removable nature of microSD cards put them at increased risk of theft.

3.2.2 Possible Near-Term Approaches

USB Security Token

Description: This approach uses a cryptographic hardware token, similar to the chip found on smart cards, in a small device that could be plugged into a mobile device's power/data connector. This would typically be a micro-USB connector, although many devices use proprietary connectors. To the mobile device, the USB security token would look like a smart card reader with an inserted PIV Card.

Availability: While commercial availability of full-sized USB security tokens is relatively high, there are few products available for use in mobile devices. Furthermore, mobile OS and application software support is very limited at this time.

Benefits: USB security tokens could be removed when not in use, and could add authentication services to mobile devices after purchase (assuming compatibility by the device and underlying OS). The token can be ported to other devices supporting USB tokens.

Considerations: USB tokens tend to be relatively small and therefore may be easily lost when removed from the handset. Usability could be a major issue. In many cases the micro-USB port is also the charging port for the devices, so USB security tokens would need to be removed to charge the device; preventing the use of the Derived PIV Credential token while charging.

UICC Tokens

Description: Universal Integrated Circuit Cards (UICC), the new generation of SIM cards, are removable cryptographic hardware tokens used by most wireless carriers to authenticate mobile devices to their networks. The UICC can also support a variety of additional applications and authentication services.

Availability: Deployment requires the cooperation of the wireless carrier, mostly likely at additional expense.

Benefits: This approach leverages a cryptographic token that will likely be found in nearly all mobile devices attached to a wireless carrier. The token may be ported to other mobile devices controlled by the same carrier.

Considerations: While technically removable, in practice users would not be able to remove the token without disabling the phone. Some mobile devices (e.g., tablets) may not have or use UICCs.

Embedded Hardware Tokens

Description: Increasingly, mobile devices are being built with embedded hardware security modules built into the device itself, either as a separate chip or built into the SoC at the heart of the device. These modules typically have the ability to securely store cryptographic keys,

including private keys, and have some cryptographic capabilities. These modules could provide for an embedded hardware token, providing authentication capabilities without adding additional hardware to the device.

Availability: While some mobile devices have a form of an embedded hardware security module, currently they are either unavailable for use or do not provide the specific set of features needed to support PKI credentials.

Benefits: An integrated solution would likely provide better user experience at a lower deployment cost. This approach could also provide unique security features not supported by other approaches (see Section 4).

Considerations: Specific approaches will depend on whatever hardware/firmware/software support is provided by individual device manufacturers and mobile operating systems. Software for managing and using credentials would likely not be portable between devices.

4. Analysis and Recommendations

Any of the options discussed above could support agency electronic authentication needs, depending on the sensitivity of data being protected and the deployed mobile devices and infrastructure. While some of the options are not supported by commercially available technology and services, current trends in the mobile ecosystem suggest these options will be available by at least some mobile devices and service providers in the next one-to-three years. As any of these options can be made interoperable with the existing PIV architecture, agencies should deploy and use the mechanisms that best meet their needs, balancing security, cost and ease-of-use. The best solutions for a particular agency may change over time, as the capabilities of mobile devices evolve.

Nonetheless, as we select, implement and deploy these solutions, we should certainly embrace the unique capabilities of mobile devices, while also recognizing their inherent constraints, in order to identify the approaches that will serve us best in the long-term. We need to be cognizant of the user experiences of these approaches, as users tend to work around even the most technically sound security mechanisms if they impede their ability to get their jobs done.

It is not practical to restrict the approach to electronic authentication in mobile devices to previous policies for desktop and laptop personal computers (PCs). While many users, with different access privileges, often share PCs, mobile devices are rarely shared, and people increasingly carry smart phones wherever they go. In a world of just PCs and flash card physical access control, it was logical to consolidate all credentials into a single PIV Card. In a world with individual mobile devices, often more than one per person, it's more logical for each device to have its own credentials. While this may sound like a major deviation from the PIV Card, this would still be re-using the same PKI infrastructure and building upon the trust and identity-proofing that was already performed to issue PIV Cards to millions of Federal employees and contractors. This is more of an evolutionary approach than a revolutionary one.

As mobile device vendors compete and innovate in this industry, we have seen them integrate an increasing number of features, including security features, into the mobile operating system, firmware, and underlying hardware. This trend will almost certainly continue, and is one of the great opportunities for success in this space. Use of Derived PIV Credentials in mobile devices, integrating the protection and use of these credentials into the lower layers of the mobile device software/hardware stack, will provide capabilities, features, and security benefits that we don't have today.

Currently, compatibility and commercial availability for any of the hardware-based approaches identified in this paper is quite limited. The only approach discussed offering broad compatibility and relative ease-of-use is the use of software tokens, essentially emulating the functions of the

PIV Card in software running on mobile devices. This approach provides the same identity assurance as PIV Cards in every respect except one: software does not protect credentials' private keys as well as hardware-based tokens like the PIV Card. While this provides a lower assurance of identity than the PIV credentials in hardware-based tokens like the PIV Card, it likely provides sufficient security for many applications and environments, given the sensitivity of most data accessed from mobile devices. While data being accessed from mobile devices is increasing, the most common IT resources accessed from mobile devices are e-mail, calendar and contact lists.

In the longer-term, federal agencies should look to adopt hardware-supported security mechanisms in mobile devices, such as the Roots of Trust identified in NIST SP 800-164, *Guidelines on Hardware-Rooted Security in Mobile Devices*. Use of security tokens embedded in the hardware of the mobile device can support stronger assurance of identity.

In reality, there is a spectrum of choices between solutions based entirely in software and those based entirely in hardware. While dedicated hardware solutions, like those envisioned in Section 3.2.2, are not commercially available at this time, many mobile devices on the market do provide hardware-backed features that can protect keys of credentials that are stored on mobile devices. Typically these features can protect keys using hardware-based mechanisms, but a software cryptographic module uses the key during an authentication operation. This hybrid approach provides many security benefits over software-only approaches, and should be used whenever supported by mobile devices and applications.

The tighter integration of the security token holding the credential's private key and the device itself presents many usability and, perhaps paradoxically, security benefits. The major usability benefit is quite clear: the user does not need to use special card readers or tokens separate from the device in order to access information. The security benefits are less clear on the surface, but equally compelling. Once users unlock the private keys on the card, the keys are at the mercy of the machine into which the card was inserted. The card has no context for whether it should be performing the actions requested by the machine. If malware is present on that machine, malware could use the private key. Closer integration with the device could provide the token greater insight into context. It could, for instance, be tied to the state of the device, only being available for use if the operating system and firmware have not been tampered with. The mobile device could also confirm authentication and digital signing operations with users, showing a message on the screen with certain transaction details (a property sometimes called "What You See Is What You Sign"), which can help detect misuse of a credential. These properties are not achieved with PIV Cards as they are implemented and deployed today.

The M-07-16 [M0716] security requirements for protecting personally-identifiable information (PII) should be reconsidered in light of mobile device technology developments, such as hardware-supported security features, the always-on, always-connected nature of the devices, and the continued pace of innovation. The "Control Remote Access" provision of M-07-16 requiring two-factor authentication, where one factor is separate from the device, is not consistent with several Derived PIV Credential approaches described in this paper that make use of security features and capabilities built into mobile devices. Electronic authentication policies will need to be updated in order to give agencies the flexibility they need to take advantage of these technologies.

5. A Look at the Future

Current technology trends point to a convergence of laptops and tablets, with those systems inheriting many of the capacities and constraints of mobile devices. In the future, the desktop computer may become less important as we conduct more of our daily business on mobile

devices that continue to become more and more capable. The decisions we make today on electronic authentication on mobile devices will likely become the de-facto required authentication mechanisms of the future.

In many ways mobile devices are in their adolescence. While they are highly capable devices that are challenging the normal ways of doing business, we are still learning how to control and manage these devices, sometimes failing to fully understand their true potential. Yet it is clear they provide a glimpse at what the future will bring.

At the time of HSPD-12 and PIV, a natural assumption was that the one thing that government employees would always have with them while working was their identity token. Moving forward, it is easy to imagine a future where the one thing carried everywhere is a smart phone. It is already true for many Federal employees, either in their personal or professional lives. Thus, it is natural to question what role mobile devices, or smart phones in particular, may have as an authentication token itself.

For the foreseeable future, we should expect a need for an identity token to support physical access control, and there are many benefits to implementing such as card as we have done with PIV. Furthermore, there is large set of infrastructure and computers currently deployed to support and use PIV. There's little reason to replace such a capable authentication token. Nonetheless, we see devices and environments that are not well suited to the use of PIV Cards. For instance, consider small, lightweight laptop computers that lack integrated smart card readers. In these cases, we can imagine using our smart phones with our laptops, employing the PIV credentials in the phones to authenticate ourselves from our laptops. Alternatively, we can imagine using our next-generation mobile phones with NFC for physical access where we would use our PIV Cards today.

While such approaches may have long-term cost or usability benefits, it would place a great deal of trust in the mobile device itself. These ideas should be considered and pursued cautiously, and only after we have assured ourselves in the security of the mobile devices that would support these use cases.

6. Conclusion

This document analyzed several current and near-term approaches for authentication from mobile devices, such as smart phones and tablets. These approaches leverage the current investment in the PIV infrastructure for electronic authentication. They also build upon the solid foundation of well-vetted and trusted identity of the PIV cardholder – achieving substantial cost savings by leveraging the identity-proofing results that were already performed to issue PIV Cards. However, in order to accommodate mobile devices, and benefit from their unique security features and capabilities, this document considered a number of approaches that use alternative form factors for the authentication tokens. Any of the options discussed in this paper could support government security and interoperability requirements, however current trends in the mobile device ecosystem argue for a flexible approach to authentication from mobile devices that leverages security features built into these devices.

When computers were too bulky to carry around most of the time, and were often shared with others, it was logical to consolidate authentication credentials into a separate token. However, the always-on, always-connected nature of mobile devices, combined their use by typically a single person, argues for each device to have its own credentials. Closer integration between the authentication credentials and mobile devices can provide a better, more convenient experience for users while also supporting security features not found in approaches that use a separate PIV Card and reader. In particular, closer integration with the device could support mechanisms

designed to detect or prevent the misuse of PIV credentials. Moving forward, as mobile devices increasingly work their way into the daily lives of Federal employees, we can continue to consider other ways to leverage mobile devices to support identity management.

Appendix A—Acronyms

BYOD	Bring Your Own Device
HSPD	Homeland Security Presidential Directive
IT	Information Technology
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
PC	Personal Computer
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PIV	Personal Identity Verification
SIM	Subscriber Identity Module
SP	Special Publication
SoC	System on Chip
USB	Universal Serial Bus UICC
UICC	Universal Integrated Circuit Card

Appendix B—References

[FIPS201] Federal Information Processing Standard 201-2, *Personal Identity Verification (PIV) Federal Employees and Contractors*, August 2013.

[M0716] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, OMB, May 2007.

[SP800-63] NIST Special Publication 800-63-2, *Electronic Authentication Guideline*, August 2013.

[SP800-157] Draft NIST Special Publication 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, March 2014

[SP800-164] NIST Special Publication 800-164, *Guidelines on Hardware-Rooted Security in Mobile Devices*, October 2012.