NISTIR 7867 rev. 2012

Usability of PIV Smartcards for Logical Access

Emile Morse
Mary Theofanos
Yee-Yin Choong
Celeste Paul
Aiping Zhang
Hannah Wald

http://dx.doi.org/10.6028/NIST.IR.7867

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

NISTIR 7867 rev. 2012

Usability of PIV Smartcards for Logical Access

Emile Morse
Mary Theofanos
Yee-Yin Choong
Celeste Paul
Aiping Zhang
Information Access Division
Information Technology Laboratory

Hannah Wald
Booz Allen Hamilton
McLean, VA

http://dx.doi.org/10.6028/NIST.IR.7867

August 2012

U.S. Department of Commerce
Rebecca Blank, Acting Secretary

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

TABLE OF CONTENTS

List of Tables and Figures

NOTES

This manuscript is being revised to correct an error in the original regarding the specific certificates on the PIV card. The corrections are in two paragraphs of **Section 4.2.5** ("Certificates"). This version supersedes the version published in June 2012.

EXECUTIVE SUMMARY

Homeland Security Presidential Directive 12 (HSPD-12) requires all Federal agencies to standardize and enhance the security of their facilities and information resources by adopting a secure multi-factor authentication (MFA) system [16]. This system employs personal identity verification (PIV) cards (a type of smartcard) and personal identification numbers (PINs). The cards are to be used for federal employee, associate, and contractor identification; physical access to federal facilities; and logical access to federal information systems. Specifications for the PIV cards and associated organizational systems are described in FIPS-201 [10]. Such PIV cards have already been widely deployed across Federal agencies (to 89 % of the Federal workforce as of the end of 2011 [12]), including the National Institute of Standards and Technology (NIST).

This report presents the findings of a usability study by NIST's Visualization and Usability Group that examines the usability aspects of smartcards mandated by HSPD-12, as well as users' perceptions and behavior regarding smartcards. We were interested in how users would use smartcards in their everyday work processes; how their work processes might change to accommodate smartcard use; and finally, the benefits and drawbacks they perceive in using smartcards for authentication.

We recruited 24 participants from a group of 100 NIST employees who were participating in a PIV technical pilot conducted by the office of the OCIO. For 10 weeks during the summer of 2010, we collected information on their experiences with using PIV cards on a daily basis for logging into/out of computers; encrypting and digitally signing messages; and authenticating to certain applications. Our study employed ethnographic methods including diaries, surveys, interviews, and field observations.

Users described to us the issues they experienced while they integrated PIV cards into their work processes, including forgetting smartcards in readers, forgetting to use smartcards to authenticate, and difficulty understanding digital signatures and encryption. The greatest perceived benefit was the use of an easy-to-remember PIN instead of complicated passwords. The greatest perceived drawback was the lack of smartcard-supported applications. Most participants had a positive experience using smartcards. Their perceptions were influenced by personal benefits experienced rather than an increase in security.

Our study findings provided us with some insights into how organizations can reduce the drawbacks and maximize the benefits of smartcards for their user population. In general, security must be as transparent as possible and maximize direct benefits to users. In order to both increase the effectiveness of security measures and make them more usable, security should be considered a feature of a well-designed system that maximizes benefits to users.

1. INTRODUCTION

Homeland Security Presidential Directive 12 (HSPD-12) defines requirements for a standardized, U.S. Government-wide identification mechanism for a reliable identification credential to be used for gaining authorized access to federal facilities and federal information systems. Personal Identity Verification (PIV) [16] is a smartcard-based multi-factor authentication (MFA) mechanism designed to increase security of government resources. The PIV smartcard contains information to identify and authenticate the cardholder, such as his full name and agency; public key infrastructure (PKI) certificates for authentication, encryption, and digital signatures; and biometrics such as fingerprints and a photo in the form of minutia templates.[1] It can be used for physical building access, for information system authentication, to support PKI, and as an identity card. Smartcard-based authentication is recognized as being one of the most secure authentication mechanisms currently available [3].[2]

To realize the full benefits – security and otherwise – of smartcard-based PIV systems, those systems must be designed with usability in mind. To that end, the purpose of this pilot study was to understand the factors that affect user behavior and perceptions in the use of smartcards for authentication and to examine factors that affect user behavior and perceptions of security in general. We addressed three specific questions:

1. How will users use the smartcards in their everyday work processes?
2. How might users' work processes change to accommodate smartcard use?
3. What benefits and drawbacks do users see in using smartcards for authentication?

We conducted our study at NIST in the summer of 2010 in conjunction and concurrently with a smartcard operational pilot conducted by the Office of the CIO (OCIO). The purpose of the OCIO pilot was to make progress on NIST's goals of achieving compliance with HSPD-12; in particular, it was designed to evaluate the feasibility of using smartcards in combination with Personal Identification Numbers (PINs) to control access to computing resources. The purpose of this report is to summarize the observations of the usability research team, who followed a group of 24 users of PIV cards over a 10-week period. In this

[1] Minutia templates are mathematical representations of biometric image data (e.g., facial images, photographs). "Plain" images are not used due to privacy concerns.

[2] Note that not all smartcards are PIV cards: the ones mandated by HSPD-12, however, are.

report, we present our findings, issues encountered by users, and recommendations for their remediation.

The scope of the usability study was limited to tasks available with the NIST PIV card implementation, such as logging into/out of and locking/unlocking a computer; encrypting/decrypting and digitally signing e-mails or documents; and authenticating to several PIV-enabled web applications. In the case of the web applications, all participants who were permanent NIST employees (not contractors) were able to authenticate to an application to register visitors to the NIST campus: the other available applications depended upon the participants' job roles (see **Section 3.1**).

The PIV smartcard affects millions of U.S. Government employees and contractors, and its use is mandated by policy. As usability specialists, we are concerned how this additional authentication factor will impact the perceptions, behaviors, and work processes of so many users. The PIV smartcards are meant to be used throughout the day as often as passwords would be used. This makes smartcard use very different from other types of card scenarios users may have experience with, such as weekly use of an Automatic Teller Machine (ATM) card. This is one of several reasons why we studied user behavior and perceptions using smartcards. Although PIV systems have the potential to be more secure than usernames and passwords, that potential can only be realized if the system is accessible and appealing to its user population.

2. PREVIOUS PIV STUDIES

A number of smartcard authentication systems similar to the PIV infrastructure in place at NIST are already in use elsewhere. One example is the European national electronic identity (e-ID) card [1] that stores different types of cardholder credentials depending on the requirements of the issuing country. Another is the Biometric Logical Access Development and Execution (PKI/BLADE) card used by the U.S. Department of State as an employee identity card and authentication token [4][17]. Also, the U.S. Department of Defense uses the Common Access Card as a military identity card, Geneva Conventions Identification Card, and authentication token [4].

While work has focused on smartcard security weaknesses such as problems with the embedded chip and PIN mechanism [9] and PIV implementation standard [5][6], very little work has looked at smartcard usability [14]. Proctor et al. [13] compared multiple authentication methods through formal task analysis. They warn that the physical manipulation of a smartcard in the authentication process can add complexity to the authentication task and reduce ease of use compared to other authentication methods.

Braz and Robert [3] conducted a comparative analysis of different authentication methods. They compared methods such as passwords, smartcards, fingerprints, and keystroke patterns on qualities such as benefits, drawbacks, security, and usability. Overall, they found that the smartcard rated as one of the most secure and usable methods for authentication.

Baldwin and Malone [2] described the use of smartcards in a health management system. The ability to store medical history and insurance information increased the usefulness of smartcards for authentication beyond being a token. Patients identified themselves by presenting the smartcard and providing a PIN. Visits for care and therapy were recorded on the smartcard, creating a case history. Patients paid for services and filed claims using the smartcard. The smartcard provided an easy way to identify patients and help the patients manage their health care accounts.

The U.S. Department of State analyzed the impact of the PKI/BLADE smartcard with biometric on their user base [17]. Their smartcard system allowed users to replace multiple username/password authentication credentials with a single smartcard/PIN credential. They analyzed their technical support logs to understand how the smartcard system affected user support requests [18]. Before smartcard deployment, password reset support requests averaged 25.8 % of all technical support requests per year. After smartcard deployment, password reset support requests dropped to an average of 10.6 % of all technical support requests per year.

Strouble et al. [15] conducted a survey that looked at issues concerning security, usability, and productivity effects of smartcards. They found the use of a PIN and PKI credential for MFA instead of a password improved the security of the authentication mechanism, but did not necessarily increase usability of the smartcard system. Sixty-seven percent of the participants forgot their smartcard in a smartcard reader at least once, resulting in potential security risks. Six percent of those participants had their smartcard lost or stolen, resulting in security risks, replacement costs, and productivity loss.

3. METHOD

3.1 PARTICIPANTS

Within the study population, there were 10 males and 14 females, with an average age of 47 (SEM ± 2). The distribution of education among the participants was representative of the organization (8 high school degrees; 10 college degrees; 6 post-graduate degrees). Ten participants were engaged in technical work (three of these were contractors); six were support staff (e.g. secretarial work); and eight worked in an administrative specialty (e.g.

finance).[3] Individuals in different job groupings not only had different sets of duties, but also had access to different applications (including applications that supported PIV authentication). Two participants reported having experience with smartcards before the study. The median time of participants' service at NIST was 13 years: the median time in their current positions was 4.5 years.

The NIST OCIO pilot (with which the usability pilot was associated) was a small-scale field test of NIST's PIV infrastructure, and was designed to accomplish the following prior to the planned organization-wide implementation of the system:

- Discover and address technical and procedural problems with the PIV infrastructure and associated support mechanisms;
- Catalog common smartcard-related issues likely to be encountered by end users;
- Provide hands-on training for staff responsible for maintaining the PIV infrastructure and providing technical support; and
- Estimate the impact of organization-wide PIV rollout on password management and technical support workload.

The OCIO research team recruited 100 participants for the OCIO pilot study, which would provide a sufficiently large sample population while keeping the number of users engaged in the pilot study down to a manageable size. The team recruited participants by sending out an e-mail request on the mailing lists of a few organizational units (OUs) that had close working relationships with the OCIO.[4] Recruitment in the technology pilot was designed to include test users from a representative sample of users in the institution. Because the pilot was focused on evaluating the PIV system and its support staff rather than the user population itself, the OCIO research team did not record participants' demographic information (e.g., age, sex, education level, years at NIST).

We recruited our 24 study participants by sending an e-mail requests to the participants in the larger pilot study, requesting volunteers. We used the same smartcard system as the OCIO pilot; the only difference was that our study included additional research methodologies to assess the smartcard system, and that it was user-focused rather than system-focused. Participation in both the OCIO pilot and our study was voluntary. However, all participants were aware that the smartcard system would soon be mandatory for most users within NIST.

[3] The NIST designations for these job role areas are ZP, ZS, and ZA, respectively.

[4] The OCIO research team elected to recruit from this particular population because prospective participants would be more likely to respond to the initial e-mail request, and would also be more invested in the actual OCIO pilot study.

3.2 INSTRUCTIONAL MATERIALS

Participants were e-mailed a document titled "PIV Pilot Test Scenarios User Guide" before their card readers were installed. The technicians who installed smartcard readers for participants also provided them with a paper copy. The document contains step-by-step instructions on how to perform various smartcard-related functions, such as logging into/out of a computer, digitally signing e-mail, and authenticating to certain web applications (as well as how to perform these functions without smartcards). It also describes common errors encountered when using a smartcard. The document also provides guidance on how to report unexpected smartcard-related problems or issues.

3.3 EQUIPMENT

Participants were given access to a fully functional PIV smartcard authentication system. Although we recruited from a "technology pilot," it was the system intended for institute-wide implementation. The equipment used in the usability study was also used in the OCIO pilot.

3.3.1 Card

The card used by participants in the OCIO and usability pilots was designed to meet HSPD-12 requirements for granting physical access to NIST facilities and logical access to the agency's systems [16]. The GSA Managed Service Office (MSO) issued these cards to all NIST employees, contractors, and associates starting in 2008, at which time they could be used for physical access only. The cards were issued along with PINs in anticipation of their being used for logical access. The smartcard PINs were 6 to 8 numbers long and selected by participants at the time of smartcard activation. However, because the smartcards were issued roughly two years in advance of the OCIO pilot, many participants never used their original PINs and forgot them, necessitating that the PINs be changed before the study began. In addition, an identifier field in the card was not compatible with NIST's PIV infrastructure – it consisted of a number instead of a unique login name – so study participants had to have their card re-initialized.[5]

Participants also retained their usernames/passwords for authentication. The password length policy was 10 characters at the beginning of the study and changed to 12 characters one week

[5] NIST had the option of modifying its PIV infrastructure and not changing the cards at all, but this would have made auditing access records very difficult. Modifying both the cards *and* the infrastructure would have been cost-prohibitive.

after the study began. Passwords expired every 90 days and every participant changed passwords at least once during the study.

As specified in NIST SP 800-104 [11], the smartcard included the following topographical features (shown in Figure 1) to support visual identification and authentication:[6]

- Employee photograph
- Employee name
- Employee affiliation identifier
- Expiration date
- Agency card serial number (back)
- Issuer identification (Back)

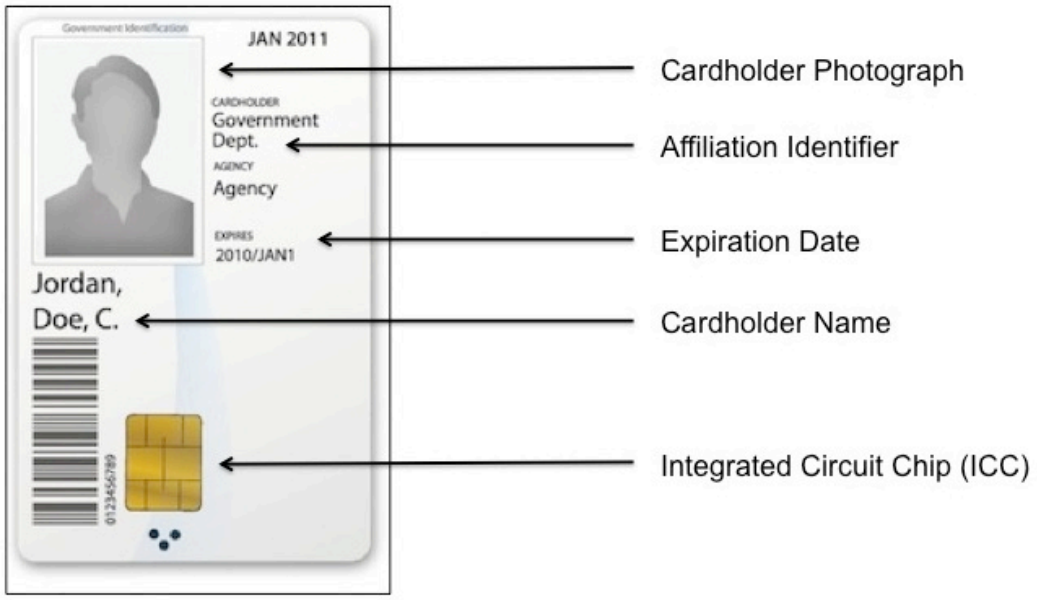

Figure 1: Schematic depicting the basic layout and required components of a federal PIV card

Each smartcard has an integrated circuit chip (ICC) containing logical credentials such as the Cardholder Unique Identifier (CHUID).These credentials can be read electronically from the card and/or used for authentication. The ICC contains biometric information consisting of a

[6] The example shown is not a NIST PIV card, but a generic mock-up of a card that complies with NIST SP 800-104.

digital image of the cardholder's face (the same as the photo displayed on the front of the card) and both of the cardholder's index fingerprints in the form of a minutia template. It also contains up to four digital PKI certificates: one certifies the validity of the card itself, while the other three are used by the cardholder for authentication (i.e., logical access), encryption, and digital signatures respectively (the last two certificates are optional).

Like employees' preexisting identification cards, smartcards could be used as physical access tokens. Participants could also use the card (in combination with their PIN and on-card PKI credentials) to log into, log out of, lock, or unlock their workstations. In addition, the card allowed them to use PKI certificates to encrypt and digitally sign e-mail.[7] Finally, they could use the smartcard to authenticate to certain web applications (such as one for registering visitors to the NIST campus).

3.3.2 Card Readers

The OCIO initially planned to issue USB smartcard readers to each participant in its logical access pilot. However, some participants had keyboards or laptops with built-in smartcard readers and used those instead, although all participants had to have ActivClient smartcard middleware[8] installed on their workstations regardless of which reader they used (see **Section 3.4** below). Of the 24 participants, 13 used the USB readers provided by the OCIO; 5 used integrated keyboard readers; and 6 used internal laptop readers (see Figure 2 below).

[7] NIST employees were able to use certain software to encrypt and digitally sign documents and messages before the smartcards were introduced.

[8] Specific hardware and software products identified in this report were used in order to perform the evaluations described. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products and equipment identified are necessarily the best available for the purpose.

Figure 2: From left to right, a USB smartcard reader, a keyboard reader, and a laptop reader

At the outset of the study, all workstations to which these readers were attached ran Windows XP with the aforementioned smartcard middleware. By the end, some of the participants had switched to using Windows 7, which has built-in smartcard functionality.

3.4 SETTING

Participants used their own computers (either laptops or desktops) and workspaces. Those with laptop computers docked the laptops at their workspaces and used external monitors, keyboards, and mice. Several participants with laptops occasionally worked from home, and several participants without laptops occasionally worked from home using their personal computers.

3.5 TASKS

Participant tasks were limited to those supported by the smartcard implementation. Supported tasks included using the smartcard to login/logout and to lock/unlock a computer, encrypt/decrypt and digitally sign an e-mail or document, and authenticate to several smartcard-enabled web applications. In each case, participants could authenticate with either their PIV cards and PINs or their usernames and passwords.

3.6 TIMELINE OF ACTIVITIES

We followed our study participants over a period of approximately 10 weeks, employing a variety of ethnographic research methods to obtain a breadth of coverage as well as a depth

of understanding of our participants. We conducted our study in three phases: Smartcard Installation, Smartcard Use, and Study Wrap-Up. See Table 1 for a summary of research activities according to the study timeline.

Table 1: Summary of study timeline and activities

Smartcard Installation		**Smartcard Use**			**Study Wrap-Up**
Pre-Install	*Post-Install*	*Daily*	*2-Week*	*6-Week*	*Exit*
Survey	Site Visit Interview Survey	Daily Diary Daily e-mail Survey	Site Visit Interview Survey	Site Visit Interview Survey	Site Visit Interview Survey

3.6.1 Smartcard Installation Phase

Before we met with participants, we sent them a Pre-Install survey, which they were asked to complete before the first site visit. The OCIO research team provided the participants with a brief training document via e-mail (See **Section 3.2**).

The technical support person then installed the smartcard hardware and software[9] and verbally guided participants through certain smartcard-related tasks, such as locking and unlocking their computers. After installation was complete, we conducted the Post-Install site visit (within 2 working days of installation, and usually sooner). We observed participants using their smartcards to log into/out of or lock/unlock their computers, interviewed them about their first-time experiences with the smartcards, administered the Post-Install surveys, and provided them the Daily Diaries.

3.6.2 Smartcard Use Phase

During the Smartcard Use phase, participants were asked to keep diaries of notable smartcard usage and events. The daily e-mail survey was sent near the end of the day for participants to complete and return. Researchers would review the daily diaries and e-mail surveys before each site visit in order to discuss any critical events during the interview, if necessary. Site visits were conducted two and six weeks after Smartcard Installation. During these site visits

[9] Some participants did not have administrative access to their workstations: in such cases, the technician would have to find someone with administrative privileges in order to install the smartcard middleware.

the researchers observed participants using their smartcards, interviewed them about their smartcard experiences to date, and administered the 2-week or 6-week surveys.[10]

3.6.3 Study Wrap-Up Phase

Study Wrap-Up activities took place 10 to 12 weeks after Smartcard Installation. Extended business travel or paid time off was not counted towards participants' total study time. This resulted in slightly longer periods of participation for a few participants. During the last site visit, we observed participants using their smartcards, interviewed them about their overall smartcard experiences, administered the Exit surveys, and collected the Daily Diaries.

3.7 DATA COLLECTION METHODS

We used four data collection methods over the course of the study: Periodic Surveys; Daily Diaries; Daily E-mail Surveys; and Site Visits and Interviews. The full versions of the surveys are available in Appendix A: Participant Surveys**.**

3.7.1 Periodic Surveys

Participants were asked to respond to the following statements in a standardized survey two or more times over the course of the study in order to evaluate their experiences with the smartcard system.[11]

1. I am **confident** I know how the smartcard works and what it does.
2. I **take the smartcard with me** every time I leave my computer.
3. Using the PIN for the smartcard is **easier than using a password**.
4. The smartcard makes the login process **easier** than the current password-based login system.
5. The smartcard makes the login process **faster** than the current password-based login system.
6. Compared to using passwords, using the smartcard is **more secure**.
7. I [**plan/will continue**] to use the smartcard.
8. I would **encourage my colleagues** to switch to the smartcard.
9. I [**am looking forward to/have enjoyed**] using the smartcard.

[10] Two of the 24 participants did not participate in the 2-week survey and interview due to scheduling conflicts.

[11] Some of these questions were re-worded or omitted in surveys issued at particular points in the study. Refer to the appendices for details.

The surveys were Word documents in which participants were prompted to enter quantitative ratings. Survey statements were rated on a 5-point scale from “Strongly Disagree” (1) to “Strongly Agree” (5) with “Neither Agree nor Disagree” (3) as neutral. Participants also had the option of providing additional comments related to each question. While the statements were framed positively and may bias responses towards the positive, we analyzed the results in terms of relative change rather than absolute value. See the appendices for the full versions of the Pre-Install, Post-Install, Smartcard Use and Exit surveys.

3.7.2 Daily Diaries

Participants were asked to keep daily written diaries of notable smartcard events. We provided notebooks for them to write in. The participants were told to write down any smartcard-related events they considered significant. Although the diaries were a data collection tool, they were primarily intended to encourage and help participants recall and think about their experiences with the smartcards. If participants were not comfortable writing in the provided notebook, they were encouraged to keep notes in an electronic document.

The participants used the written diaries in different ways, depending upon their preferences. Some participants made a note every time they used their smartcard. Others used it very little or not at all. Most used it to note critical events (e.g., forgetting the smartcard in the reader, mistyping their PIN, accidentally signing an e-mail) in anticipation of surveys and interviews. The diaries were collected during the last site visit during Study Wrap-Up.

3.7.3 Daily E-mail Surveys

The daily e-mail surveys asked participants to report about specific smartcard usage in a Yes/No format, such as “Did you use your password today?”, and also provided an area for additional comments. The purpose of the daily e-mail surveys was to supplement the daily diaries as a way of reporting critical events, and not as a quantitatively evaluated questionnaire.

3.7.4 Site Visits and Interviews

Site visits allowed us to observe smartcard use in the participant's natural environment. Interviews provided an opportunity to discuss the participant's smartcard experience since the previous visit and review any critical events that were reported in the daily diaries or daily e-mail surveys. We also administered and collected periodic surveys. We supplemented our notes from these site visits with digital recordings, which we then transcribed.

3.7.5 Post-Study Survey

At the conclusion of our 10-week study, we conducted a voluntary survey of participants in the OCIO pilot using SurveyGizmo. We asked respondents questions designed to gauge their confidence with using smartcards for various purposes (e.g., logging into/out of their computers, authenticating to web applications, encryption) and see whether they intended to continue using smartcards in the future.

4. RESULTS

We report the analysis of our study results in three sections. First, we provide descriptive statistics for the quantitative data collection methods. Second, we discuss our analysis of the qualitative data, including in-context discussion of the quantitative results. Third, we provide an analysis of the results from the voluntary SurveyGizmo post-study survey we issued to all participants in the OCIO pilot.

4.1 DESCRIPTIVE STATISTICS OF QUANTITATIVE METHODS

4.1.1 Periodic Surveys

Results from the periodic surveys are reported as mean values with 95 % confidence intervals in Table 2**.** Pairwise comparisons are discussed alongside the qualitative results. The Wilcoxon signed-rank test is used for pairwise comparisons and Kendall's correlation is used for measuring relationships. An empty cell indicates that a particular question was not included in a survey because it was not relevant at the time. Observation on the trends indicated in Table 2 are summarized below: for a more in-depth discussion, refer to **Section 4.2**.

Table 2: Survey statement with mean values and 95 % confidence intervals

Survey Questions	Pre-Install	Post-Install	2-Week[12]	6-Week[13]	Exit
I am **confident** I know how the smartcard works and what it does.	3.50 ± 0.38	4.42 ± 0.19	4.33 ± 0.30	4.12 ± 0.40	4.20 ± 0.34

[12] Two of the 24 participants were unable to take the two-week survey due to schedule conflicts.
[13] Two of the 24 participants were unable to take the six-week survey due to schedule conflicts.

Survey Questions	Pre-Install	Post-Install	2-Week[12]	6-Week[13]	Exit
I **take the smartcard with me** every time I leave my computer.	–	–	3.67 ± 0.47	4.04 ± 0.43	3.88 ± 0.41
Using the PIN for the smartcard is **easier than using a password**.	3.5 ± 0.29	3.92 ± 0.38	4.17 ± 0.28	4.24 ± 0.38	4.32 ± 0.39
The smartcard makes the login process **easier** than the current password-based login system.	3.40 ± 0.34	3.73 ± 0.39	4.08 ± 0.35	4.24 ± 0.31	4.24 ± 0.31
The smartcard makes the login process **faster** than the current password-based login system.	3.33 ± 0.33	3.50 ± 0.41	3.83 ± 0.40	3.68 ± 0.52	3.64 ± 0.49
Compared to using passwords, using the smartcard is **more secure**.	3.73 ± 0.34	–	–	3.60 ± 0.32	3.84 ± 0.29
I [**plan/will continue**] to use the smartcard.[14]	4.19 ± 0.19	4.35 ± 0.19	4.29 ± 0.38	–	4.48 ± 0.32
I would **encourage my colleagues** to switch to the smartcard.	–	–	4.08 ± 0.33	4.04 ± 0.26	4.32 ± 0.31
I [**am looking forward to/have enjoyed**] using the smartcard.[15]	3.92 ± 0.26	–	–	–	4.32 ± 0.29

As shown in the first row, participants' confidence in their ability to properly use the new smartcard authentication system increased significantly immediately after installation (Pre-install/Post-install: $W = 3.87$, $p < 0.05$) and remained high throughout the study (Post-install/Exit: Kendall's $W = 0.04$, $p = 0.41$).

4.1.2 Daily E-Mail Surveys

We collected a total of 682 daily e-mails; the average number of e-mails collected from each participant during the study for each participant was 28.4 (SEM ±2.5). The number of e-mail surveys collected diminished over the course of the study with 3.5 (SEM ± 0.2) surveys/week collected between the Post-Install and 2-Week site visits; 2.5 (SEM ± 0.3) surveys/week

[14] Wording changed from Pre-Install survey to subsequent surveys (as indicated by the options within the square brackets).

[15] Only included in Pre-Install and Exit surveys, with wording changed (as indicated by the options within the square brackets).

between the 2-Week and 6-Week site visits; and 2.3 (SEM ± 0.3) surveys/week between the 6-Week and Exit site visits. Figure 3 below displays this trend over time.

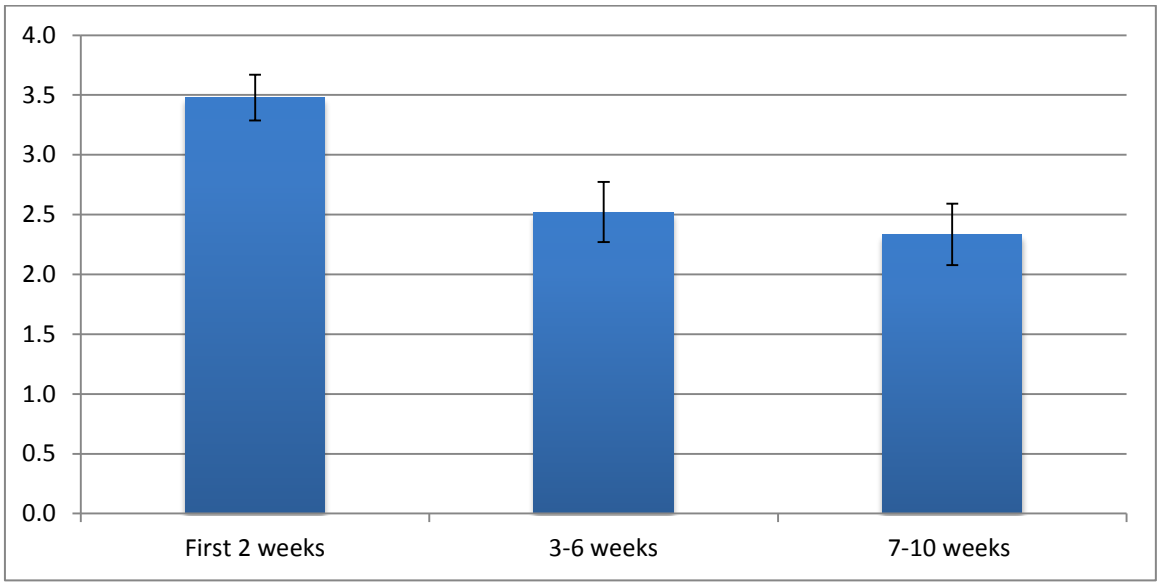

Figure 3: Average number of E-mail surveys collected from each participant over the course of the usability pilot study

4.2 ANALYSIS OF OBSERVATIONS

We took a grounded theory approach to our study, approaching the subject matter with open-ended questions rather than a hypothesis or dominant theory to prove or disprove. By using rigorous methods of data collection and analysis, we developed insights and recommendations based on patterns emerging from the data themselves (see **Section 5**) [8]. We used an application called NVIVO to code, conceptualize, and categorize qualitative data obtained from surveys, daily diaries, e-mail questionnaires and user interviews.

Table 3 provides a summary of reported issues, with discussion in the following section. Each of the factors in the table will be addressed in separate sections below.

Table 3: Summary of study observations by issue topic.

Issue Topic	Observation
User Confidence	• Confidence in using smartcards increased after Installation

Issue Topic	Observation
Smartcard Readers	• New object in environment to get used to • Reason for forgetting smartcard in reader • Form factor may matter
Using Smartcards	• Smartcards easier for authentication than passwords • Forgot to remove smartcards from readers • Forgot to use smartcards to login • Forgot to use smartcards to lock screens • Forgot to use smartcards to unlock screens • Smartcard slower to login than password but faster for other uses • Unattended smartcard message is sometimes useful
Passwords vs. PINs	• PINs easier to use than passwords • Password requirements were burdensome • Passwords became difficult to remember because of smartcard use • Various password management strategies
Certificates	• Selecting certificate for web application authentication was confusing • Certificates could not be backed up or transferred
Digital Signatures and Encryption	• Digital signatures and encryption were easy to use • Did not understand digital signatures and none would use them • Understood encryption but few would use it • Implementation does not support inter-institutional use
Security Behavior	• Smartcards gave perceived increase in security • Low understanding of how or why security works • PII users were the most security conscious
Overall Experience	• Overall positive experience with smartcards • Most would recommend smartcards to colleagues • Most would continue using it voluntarily • Some had problems fitting smartcards into work processes

4.2.1 User Confidence

Seventeen of the 24 participants reported reading the provided training materials before the smartcard hardware and software were installed. Several participants indicated that they preferred in-person training rather than reading the training documentation. One participant noted that he preferred a "*hand-holding demo*" (P3) when using a new system for the first time. Another participant indicated that she "*learn[s] better by hands-on training*" (P12). The personalized training could be a factor in the significant increase of confidence post-

installation. However, not all participants felt the need for hands-on training or instructional materials. As one participant explained, "*I prefer to jump in and just start using any new product, referring to the documentation only when I get stuck or find features I'm curious about*" (P16).

4.2.2 Smartcard Readers

Thirteen of the 24 participants used USB readers that were placed on their desks, like the one shown in Figure 2 (left). The rest used readers that were either integrated into laptops or keyboards. The location of a reader on a desk varied, as did the number of items that might obscure it from view. The reader itself added to clutter on the desk, as one participant commented, "*I know I'm going to dislike the wire connecting the smartcard reader to the computer – makes for a messy desk!*" (P7). This participant attempted to clean her desk by moving the reader out of the way, but later attributed the position of the reader to why she may have forgotten her smartcard, "*I tidied [the] smartcard reader cord - made [the] reader less intrusive, but moved it further out of [the] workspace. It may be a reason for forgetting to remove the smartcard to lock my computer.*"

Another participant also believed that his USB reader being obscured caused him to forget his card: "*I walked away at one point and forgot my smartcard. This has happened once or twice, and it makes me think that smartcard readers should probably be fairly visible*" (P14). Later that week, he tried a keyboard reader with more success: "*Switched out my [USB] reader & keyboard for a new keyboard that included a smartcard reader. I like the setup much better. Less clunky, and the smartcard is more visible.*" Besides adding to clutter on the desk, another problem with the USB reader was that it was not attached to a stable object and required participants to use two hands when removing and inserting the smartcard – one to hold the card and one to hold the reader itself. One participant remedied this problem by attaching her USB reader to her computer with rubber bands.

Not all participants with keyboards containing built-in readers like the one shown in Figure 2 (center) could use them, because their keyboards were in keyboard trays attached to the underside of their desks. Several of these participants also kept their keyboards partially hidden under their desks while they typed, leaving too little clearance for the portion of the card that sticks out of the reader. Unless the keyboard tray was completely pulled out from under the desk, it would not fit under the desk with the smartcard inserted in the keyboard reader.

4.2.3 Using Smartcards

Participants commonly reported forgetting to remove their smartcards from their readers. Thirteen of the 24 participants (54 %) forgot their smartcards in their readers at least once during the study. The most common scenario in which participants forgot their smartcards was during short trips out of their work areas, such as down the hall to visit a colleague or to use the restroom. Three of the 24 participants forgot their smartcards in their readers after leaving an access-controlled area, and had to rely on their non-smartcard identity cards to gain access to their buildings. Six participants forgot their smartcards in their readers overnight. One participant forgot her smartcard in the reader overnight and drove back to campus to retrieve the card. Three participants reported forgetting their smartcards at home and had to use their passwords to log in. Incidents where participants left their smartcards in the readers overnight or at home only occurred once or twice per participant.

Even though half of the participants reported in interviews that they forgot their smartcards in the readers at some point during the study, most participants reported remembering their smartcards most of the time by the end of the study. Many participants who forgot their smartcards in readers early in the study reported that they forgot their smartcards less often as time went on. A few of these participants pointed out that it seemed to take them about one month before they developed a habit of using and remembering their smartcards; however, this change is not indicated in the periodic survey results. One participant described a system she developed to help her remember her smartcard; when she removed her smartcard from her badge holder, she would place the badge holder in front of her keyboard. It served as a reminder for her to take her smartcard before she left the office. This participant did not report forgetting her smartcard at any time during the study.

There were several reasons why participants did not use the smartcard to log into or unlock their computers. In the beginning of the study, most participants simply forgot to use their smartcards because it was not yet a habit. This was especially true for participants who had good security habits, such as those who consistently locked their computers with the keyboard when they left their workspace. As one participant stated, *"This is going to take some getting used to - I have been using the keyboard to lock my machine for 10 years - hard habit to break"* (P21). Other reasons participants did not use the smartcard to log into or unlock their computers included because they forgot their smartcard at home, were using multiple computers at once, or were prompted to enter a username and password by the software. By default, computers running Windows XP displayed a username and password dialog instead of a PIN dialog unless the user inserted his/her smartcard into the reader, in which case he/she would be prompted for a PIN. This login dialog may have affected whether participants used their usernames and passwords or smartcards and PINs to log in. A few participants discovered that if they pressed Escape on the keyboard with their smartcards

in their readers, a PIN dialog would display. The usability research team (and participants themselves) shared this information with other participants. If participants did not use the smartcard to log in to the computer, they would not be able to remove the smartcard from the reader in order to quickly lock the computer during the same login session. This caused some confusion in the beginning of the study when participants were not yet consistently using the smartcard to log in: "*After logging in with my keyboard, I locked the machine but the smartcard could not unlock it until I logged in and locked the machine again*" (P14).

Unlocking computers also caused confusion for several participants in the beginning of the study. When returning to their locked computers, out of habit these participants would use CTRL+ALT+DEL in order to cancel the screensaver and unlock their computers. Using this key combination displayed the username and password dialog. Since participants were prompted with username and password dialogs, they entered their usernames and passwords and created sessions that could not be locked by removing their smartcards. It took time and practice for these participants to get used to using their smartcards to unlock their computers without pressing CTRL+ALT+DEL.

Nine of the 24 participants noticed that it took between 10 and 30 seconds longer to authenticate and log in to their computers using smartcards and PINs than it did using usernames and passwords. The physical act of inserting the card also added time to the login process. While the smartcard is slower in some cases, most participants considered the overall system tradeoffs and still felt smartcards were faster and easier to use: "*Unlocking when I returned to my desk was simple and no harder or time-consuming than username and password – maybe easier*" (P7).

Participants who worked both at their computers and elsewhere in their work areas often experienced automatic computer screen locking after 15 minutes of inactivity. When the screen automatically locked with a smartcard in the reader, a message describing an unattended smartcard appeared. Participants who frequently worked on other machines at their work areas found these error messages frustrating: "*It's not unattended, I'm right here!*" (P17). However, participants who accidentally locked their computers using their keyboards felt the unattended message was useful: "*The message helped me not forget my smartcard when I accidentally locked using the keyboard*" (P2).

4.2.4 Passwords vs. PINs

Many participants noted that the PIN was an important feature of their positive smartcard experience, particularly for its ease-of-use. The PIN was numeric-only while the system password consisted of numbers, upper- and lower-case letters, and special characters. In addition, the PIN never expired, but NIST password expired and had to be changed every 90

days – and since single sign-on (SSO) functionality is not available at NIST, this meant users would have to change their passwords in multiple systems and applications. The PIN was six to eight characters in length, while passwords were required to be 10 (later 12) characters long. One participant noted the importance of the PIN not changing: "*If the PIN has to be changed as often as the password, there would be a reduced benefit to having the PIN*" (P21). Password length had a noticeable effect on participants' perceptions. Several participants complained that the new 12-character password requirement instituted during the course of the study made it more difficult to remember their passwords.

The password length requirement was not the only burden passwords placed on participants. Smartcard use prevented participants from practicing their passwords as often as they did before the study. Several participants felt they risked forgetting their passwords: "*It is an effort remembering my system password*" (P15). Some participants needed their primary network password to log into computers that were not smartcard-enabled, providing an opportunity to practice their passwords if they were synchronized. However, participants who did not synchrnoize passwords or used their passwords only to log into their computers were at a greater risk for forgetting.

Participants also described various methods they used to manage passwords before their experience with smartcards. Nine of the 24 participants reported managing their passwords by recording them on paper and storing them in their wallets, purses, or drawer in their offices. Some participants also attempted to re-use the same password for multiple applications so they had fewer passwords to remember. However, not all password requirements were the same and it was easy for their passwords to get out of synchronization. It was also extremely inconvenient to retrieve a password for every account. Two participants reported using software to save and manage passwords. Some participants viewed the smartcard as a move towards an organizational SSO solution (which, as previously mentioned, is not widely implemented at NIST): "*The idea of having one "PIN" for all applications is a dream come true! Also - less work for both user and the IT help desks for resetting passwords!*" (P18).

4.2.5 Certificates

Several web applications included support for smartcard-based authentication. Participants authenticated to web applications by visiting the login page, where a browser dialog appeared asking participants to select a certificate to use for authentication. For web application authentication, the certificate used for authentication did not matter. However, the authentication process was different depending on which certificate participants chose, and different Internet browsers did not display the list of available certificates in the same way. If participants chose the non-repudiation digital signature certificate, they were asked to

enter a PIN. If participants chose the authentication certificate, they were not asked to enter a PIN if they had already entered a PIN in the last 15 minutes. However, without expert knowledge in certificates, it was difficult for participants to distinguish the non-repudiation certificate from the digital authentication certificate.

The smartcard authentication system also does not allow users to back up their private keys (for encryption and digital signatures) on their card or save/transfer them. Three of the 24 participants expressed concerns about the lifetime of certificates used to encrypt e-mail and documents. If a smartcard is lost, stolen, expires, or is replaced, certificates are lost forever. Previously encrypted e-mail and documents can no longer be decrypted and the information will no longer be accessible. One of the participants, who worked with financial information, was concerned that he would not be able to access encrypted data that needed to be available for auditing.

4.2.6 Digital Signatures and Encryption

The most infrequently used smartcard features were digital signatures and encryption. Once familiar with the smartcard's functionality, participants were comfortable with digitally signing and encrypting e-mail and documents and found both easy to use. However, most participants did not know when to encrypt or apply a digital signature to an e-mail or document, even after reading the sample use cases in the training document and after discussions with researchers during interviews. The training documentation explained how to sign and encrypt, but not why a participant would want to do so. No participants indicated a need for signing e-mail or documents, although several participants routinely tested those features. Several participants stated they would not consider using signing and encrypting unless it were required by policy: "*I see no value in a digitally signed e-mail and would do so only if I was required to*" (P23). Two of the 24 participants used encryption to send passwords through e-mail, and found it useful. The few participants who considered using signing and encrypting were those who already used some type of signing and encrypting in other applications before the OCIO pilot.

All participants unintentionally signed e-mail at some point in the study due to a technical problem that temporarily changed an option in their e-mail clients and made them apply digital signatures by default. While most participants immediately noticed a difference in behavior and found typing a PIN for every sent e-mail inconvenient, one participant decided to experiment with e-mail signing for the rest of the study. This participant did not find digital signatures a huge burden, but he was also a technical user who understood the purpose of digital signatures. He also acknowledged that the digital signature functionality might not be for everyone: "*I send a small number of e-mails on a typical day, so it isn't a big deal for me, but if I had to enter [the PIN] 50 or 100 times a day, it would become bothersome*"

(P21). Few participants could describe a practical use for digital signatures. One participant expressed his doubts about the usefulness of digital signatures for non-repudiation: "*I don't see the point. People are going to know who I am based on what I say in the e-mail*" (P2).

Participants who worked regularly with personally identifiable information (PII) considered the possibility of signing and encrypting e-mail or documents, but in practice found it impossible to use with the current smartcard implementation. Within the workplace, coworkers shared PII through secure applications, shared files on a shared remote storage location, or paper. Sharing PII out of the workplace with external contacts was the most common scenario where encryption would be useful. However, a participant could not encrypt a message to another user or verify that user's signature unless they had the user's public certificate. There was no infrastructure to easily obtain, share, and verify certificates from contacts outside the institute. Several participants explained how they thought encryption would be more useful once they knew their colleagues outside the institution had an infrastructure that supported certificate sharing.

4.2.7 Security Behavior

Many participants commented that they felt the smartcard was more secure; however, reasons why they felt the smartcard was more secure varied. For some participants, using the smartcard "*enforces good habits*" (P14) and encouraged participants to lock their computers. As one participant said: "*I felt my computer was more secure than ever before because I was forced to secure my computer each time I left my office by taking my smartcard with me each time*" (P15). At the same time, one participant who had already developed good computer locking habits was afraid that the smartcard had negatively impacted how often she locked her computer in the beginning of the study.

While participants felt the smartcards were more secure, few could articulate how or why. Three participants explained the smartcard was an additional security factor. Two participants noted the smartcards increased security because they would be difficult to crack or copy. Participants had mixed feelings about the use of a PIN instead of a password. Some participants felt that the shorter PIN was a benefit because the PIN is easy to remember and security would increase because it would not need to be written down (since, unlike a password, it did not need to be changed periodically). However, one participant was concerned that the PIN was not complex or long enough and might pose a security risk, "*The PIN for the smartcard is all numeric & 6-8 digits. Not sure if the multi-factor aspect makes it more secure than 1 more complex password alone*" (P23). This participant's understanding of smartcard-based authentication was faulty – hence the concern about a short PIN being less secure than a long password – but not unexpected, given that the participant is not a security expert and is thinking in terms of password-based authentication.

At the beginning of the study, several participants described themselves as being very diligent about security. Participants who seemed to have the best security habits, such as consistently locking their computer screens when leaving the office, were those who worked with PII or financial data. These participants were very aware of the sensitivity of the information they worked with, and felt that most security measures were justified. Participants who did not share these job roles had very different attitudes toward security. There seemed to be a high amount of inter-office trust, i.e. coworkers were not the threat. Two of the 24 participants indicated they left their smartcards near their readers when they temporarily left their workspaces. One of these participants attempted to justify this behavior: "*It is OK since no one can get to my computer without the PIN and my other card can get me in the building.*" (P18). Although this participant was warned that her non-smartcard identity card would be phased out – meaning she would have to rely on the smartcard for physical access – she did not consider this when she developed this behavior.

4.2.8 Overall Experience

Even though each participant reported at least one problem or issue regarding smartcard use during the study, the overall satisfaction of participants at the end of the study seemed positive. All but three of the 24 participants (88 %) indicated during the exit interview that they would recommend the smartcard to their colleagues. In general, participants were positive about using the smartcard, especially those in administrative job roles. These participants used the smartcards to access multiple applications and described a noticeable benefit.

Overall, participants were very positive about continuing their smartcard use after the study. However, not all participants had a consistently positive experience with the smartcards. Bad experiences and general frustration with the smartcards seemed to have an effect on some participants' behavior and perceptions. While minor problems, especially at the beginning of the study, were expected and accepted by most participants, issues that were persistent and affected work productivity were not acceptable. Early frustration with the smartcard had noticeable effects: "*Off to a bad start today and never fully recovered. I didn't use the smartcard for most of the day*" (P7). Although this participant had a particularly frustrating day, she resumed using the smartcard the next day and reported positive comments about her smartcard experience during the exit interview.

Another participant could not find a way to fit smartcard use into her existing work process. The smartcard authentication was noticeably slow to her and she described being "*always in a hurry to log in*" (P24). She explained in the exit interview that if the smartcard became policy, she would use it; however, there were not enough benefits to encourage her to continue using the smartcard voluntarily. This benefit tradeoff was discussed by another

participant who shared the same sentiments about recommending the technology, "*I can't really recommend it, as it has few clear benefits to offset the downsides*" (P23).

4.3 POST-STUDY SURVEY

After the study was completed, we developed and deployed a voluntary web survey using SurveyGizmo. The OCIO PIV pilot lead sent mail to all 100 participants requesting their participation. Of the 24 usability pilot participants, 20 completed the post-study survey; 21 of the 76 other pilot users did so. The response rate for the usability pilot testers was 77 % and for the other pilot testers was 28 %. The difference in response rate is highly statistically significant ($p < 0.01$). This difference in response rates may be attributable to the Hawthorne effect [7].

Table 4 describes some characteristics of the two groups. Numbers in columns may not add up to the total number of participants in a group since people were free to decline to answer any question. The composition of the groups of responders was roughly equivalent with respect to the attributes shown in the table.

Table 4: Characteristics of web survey participants

Attribute	Value	Usability pilot testers	Non-usability pilot testers
Gender	Female	12	9
	Male	8	11
Age	18-24	1	0
	25-34	2	3
	35-44	6	4
	45-54	7	9
	55-64	4	4
Career Path	Administrative	5	5
	Technical	9[16]	12
	Support	4	2
	Contractor	2	1
Education	High school	2	1
	Some college	5	2
	Associate's or Technical degree	1	1
	Bachelor's	6	9
	Master's	6	6

[16] According to the demographic survey conducted at the Pre-installation visit, there were only 7 technical personnel. The reason for the discrepancy seen in the web survey is uncertain.

Attribute	Value	Usability pilot testers	Non-usability pilot testers
	Post-graduate	0	1
Reader type	External USB	13	12
	Keyboard	3	6
	Internal laptop	5	9
OS	XP	19	19
	Vista	0	1
	Windows 7	2	3

We also asked participants about their perceptions of and experience with smartcards following the pilot studies, and discovered the following:

- Of 41 respondents, 11 reported routinely using more than one computer at a time.
- 16 of 41 reported that they used a remote desktop.
- More usability group participants than other OCIO pilot testers found the PIV system easier to use than usernames and passwords (17/20 vs. 10/21). Mean values on a 5-point scale were 4.2 and 3.5, respectively ($p < 0.05$ by Mann-Whitney U).
- When asked whether PIV authentication is more secure than username/password authentication, there was no difference between the average responses of the two groups (3.75 for usability testers vs. 3.86 for others: p=NS).
- We asked people about the kinds of things they used PIV for and about their confidence in using the card and reader to do them. The results are shown in Table 5. Usability testers registered more visitors and, not surprisingly, they were more confident in doing this. Otherwise, there were no notable differences between the groups.

Table 5: Comparison of the frequency of use of functions between pilot groups

	Number saying they have done activity		Confidence	
Activity	**Usability**	**Non-Usability**	**Usability**	**Non-Usability**
Register visitor	13	7	4.3	3.9
Encrypt	16	14	4.3	4.0
Digitally sign	15	15	4.3	4.0
Web Application	9	6	NA	NA

In response to the question “How often do you use your PIV card to login or lock/unlock your computer?”, 15 participants in the usability study said they used their card “most of the time,” while only 9 non-usability participants did (see Figure 4).

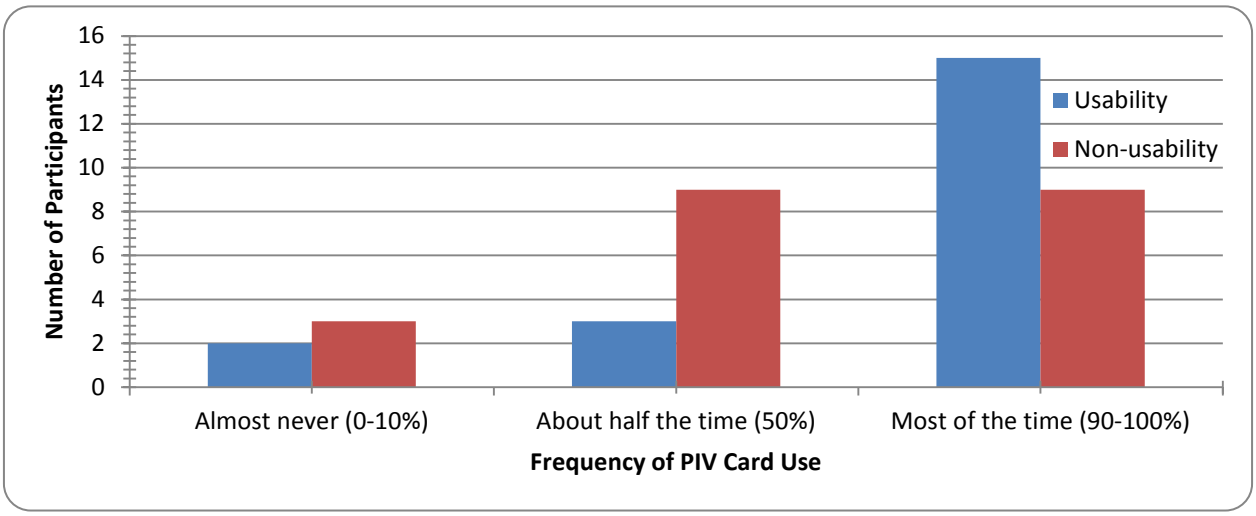

Figure 4: Frequency of PIV use for access

Participants frequently reported forgetting cards during interviews, so we asked about this during the web survey. There were no differences between the usability and non-usability groups. Respondents to the post-study survey reported misplacing or forgetting their card in one or more of the following ways during the study:

- 6 left their card at home by accident;
- 10 left their card in their reader overnight;
- 29 left their card in the reader unintentionally during the day.

The final questions on the survey looked at user acceptance. We asked two ”Yes/No” questions to get at this issue. The first of these asked about whether participants intended to continue using their PIV cards. See Table 6 for a summary.

Table 6: Intentions of usability and non-usability pilot participants regarding continued PIV use

Now that the PIV Pilot Study is completed, I will...	Usability	Non-usability
... continue to use my PIV card for all PIV-enabled logins	15	8
... use both my PIV and usernames and passwords	4	7

Now that the PIV Pilot Study is completed, I will...	Usability	Non-usability
... continue to use my PIV card for all PIV-enabled logins	15	8
... go back to using only usernames and passwords	0	2
I am not sure what I will do	0	4

All the usability participants said that they planned to continue to use their cards for accessing their computers at least some of the time. The non-usability survey respondents are less committed to continued use.

The second question asked: "Would you recommend the PIV card and reader to your colleagues?" All but 1 usability participant and 2 non-usability participants answered "Yes" to this question.

5. DISCUSSION

The goal of our study was to understand factors that affect user behavior and perceptions in the use of smartcards for authentication and to examine factors that affect user behavior and perceptions of security in general. We discovered a variety of usability issues related to smartcards, which we have grouped into four categories: Installation and Training; Work Environment and Form Factor; PIV Card and Reader; and Overall Acceptance.

5.1 INSTALLATION AND TRAINING

The installation process was designed by the OCIO pilot team to simulate the process that NIST users would be expected to follow during actual PIV card and reader roll-out. This design required the involvement of groups outside the direct control of the OCIO pilot team and pilot users. For example, the Security Department was responsible for updating PIV badge certificates and the Desktop Support Team was assigned the task of performing the actual installation of the reader on the users' desktops. The involvement of multiple teams who often had little or no coordination between them – and, at this early stage, a lack of experience with PIV technologies – sometimes caused logistical issues.

5.1.1 PIV Certificate Update Process

The first step for users was to update certificates on their PIV badge. Even though each employee had been issued a PIV card prior to the OCIO pilot study, the cards – originally

initialized by GSA – are not compatible with NIST's PIV infrastructure. The current process for certificate updates requires each staff member to visit the Security Office at least once, but most people will need to visit twice – once to reset their PIN (if they forgot the one they were assigned when they initially received their PIV card) and once to actually get the updated certificates.

On several occasions staff members were "updated" with bad certificates due to an issue with the software used to re-initialize the card. This required repeat visits to Security after iTAC identified the problem during an attempt to install a reader and the requisite middleware. It also required the affected user to reschedule installation. The problem was pervasive and appeared to involve about 30 % of our users. A process that should have required about 30 minutes from a user, 5 minutes from Security staff, and 30 minutes for the installer ended up taking twice or even three times that long. Often our participants reported that when they asked the Security person whether he was sure the card was fixed, they were told to check it if they knew how: Security personnel had not been instructed on how to check if a card was valid. A few of the more technical users actually managed to use the software in the Security office to inspect their certificates to determine whether the process had worked.

The certificate update process was critical not just from a PIV functionality perspective, but also from a user perspective, as it provided participants in the OCIO and usability pilot studies with their first impression of smartcards. For a significant number of users, this first impression was decidedly negative, and not helpful in terms of promoting their acceptance of smartcards.

5.1.2 Technical Support

The study design identified iTAC and Desktop Support as the organizations responsible for deployment. ITAC's role was to contact pilot users to schedule reader installations, mediate problem reports from users, and coordinate with Desktop Support. Desktop Support would push smartcard middleware to users' computers and perform installations. In several instances, scheduled installation sessions had to be cancelled because iTAC and Desktop Support had no permission in several work groups to perform software installations. We discovered that iTAC is not the sole point-of-contact for desktop system maintenance. Some work groups had their own local, specialized IT support staff, who often held administrative rights to the computers for which they were responsible. The OCIO pilot team had to locate and coordinate with these local IT support units in order to perform smartcard middleware installations on some participants' computers.

In addition, users did not always contact iTAC when they experienced trouble with the PIV system. The post-study survey of all usability pilot users asked participants to list the types of PIV-related problems they encountered and indicate how they attempted to resolve those

issues. It is important to note that all pilot testers were instructed to use their usual mechanism to resolve problems – if they would usually contact iTAC, read documentation to figure out a solution themselves, or ask a colleague, then they should do that when PIV issues arose. Despite these instructions, nearly one-third of respondents reported that they called the OCIO test lead to report problems. Only five respondents to the post-study survey said that they called iTAC regarding PIV-related issues.

As our experience demonstrates, any organization with partially or completely decentralized tech support makes the job of rolling out any software and/or hardware more complex: in such environments, it is difficult for those implementing PIV systems to identify and coordinate with those who are responsible for maintaining local machines. This not only causes frustration to users in and of itself, but makes problems with the PIV system more difficult and costly to detect and resolve – thus creating a negative impact on users (and the organization) down the road as well.

5.1.3 Training: Documentation and Teaching Methods

Most users received training from the technician who installed their card reader. In practice, this was limited to inserting and removing the card, logging in, and locking the screen by removing the card. Additional functionality of the PIV card such as encryption and digital signing was described in a document called "Test Scenarios and Instructions" which was sent by the usability pilot lead to each participant by e-mail in early May. During our first meeting with each participant, we asked about the training document. Seventeen of our 25 participants reported at least leafing through the document when they had received it. Five people could not remember receiving it at all. On the post-installation survey, participants rated the materials on a 5-point scale and gave them an average of 4.04, showing a positive opinion.

Several participants said that they preferred to learn to use new technologies just by "jumping in" and experimenting. Others preferred a hands-on demonstration to help them ensure they were using the card and reader correctly. These observations indicated that what constitutes "good training" varies on an individual basis; there is no one training method that will be most effective for everyone.

5.2 WORK ENVIRONMENT AND FORM FACTOR

Form factor pertains to the size, shape, and design of an object. In this case, the objects at issue are the PIV card itself and the different types of readers participants used during the study.

As mentioned in **Section 3.3.2**, three types of card readers were used during the usability pilot: an external USB device, an integrated keyboard reader, and an internal reader on laptops. We observed users of all three types of systems while they worked in their usual workspace environment. We discovered that some users experienced ergonomic and placement issues with the cards and with USB and keyboard readers. Most importantly, we discovered that there is no single "ideal" PIV card reader that will work for all users.

5.2.1 PIV Cards

Hands that were damp or moist made removing the PIV card from the badge holder difficult. Since working with the badge holder was perceived as difficult, some users resorted to storing the card in a pocket or to leaving it on the desk next to the reader. Neither of these solutions is optimal since both prevent the card from being used as an ID badge.

5.2.2 USB Readers

USB readers like the one in Figure 2 (left) require 2-handed operation: since the reader is not anchored to anything, the user must hold the smartcard in one hand and the reader in the other. Some users observed that the need for 2 hands made the use of the card take longer than using a username and password. A participant with limited wrist mobility failed repeatedly when attempting to insert the card into the reader. Although the user could insert the card, the twisting motion that was used to accomplish this prevented the reader from registering the card. A few users remedied the problem by either taping or tying their reader in a stable location.

Often the USB cable ended up snaking across a user's work surface. One user "solved" the problem by winding up the cable and putting the card reader near the USB hub. This resulted in the card being about 3 feet away from the user to the far left, where it was not easily visible. The participant started to forget to remove the card when leaving the office. She was not the only one with this problem: quite frequently we observed users hunting for the USB reader on their desktops. Even a small amount of clutter made it easy to lose track of the device. Also, users often reported that when their card was in their USB reader it was hard to notice. They wanted something located in the near periphery of their visual field.

5.2.3 Keyboard Readers

When a smartcard is inserted into an integrated keyboard reader, as seen in Figure 2 (center), a significant portion of the card sticks upward. Some users kept their keyboards in pull-out trays attached to the underside of their desks. These trays interfered with the upper edge of the card, especially since some users routinely use the keyboard while it is partially pushed under the work surface. One of these users replaced his keyboard reader with a USB reader

to allow him to continue to work in his usual manner. Several users of a keyboard reader reported wear and tear on their PIV cards. Dark lines and depressions along the point of contact were excessive compared to users of USB readers.

5.2.4 Laptop Readers

Laptops with built-in readers, like the one in Figure 2 (right), appeared to be relatively problem-free. This was true for systems that were used off-site for telework or travel as well as for systems that were docked while on-site.

5.3 PIV CARD AND READER IN USE

The everyday experiences of participants in the usability study provided the usability research team with some valuable insights into how they adjusted to using smartcards and PINs instead of usernames and passwords (and how they compared the two once they had grown accustomed to smartcards). Participants also highlighted some logistical, technical, and organizational policy issues related to smartcard use at NIST.

5.3.1 Forgotten, lost, or stolen PIV cards

Three-quarters of the people responding to the final web survey reported leaving their PIV cards in their reader unintentionally during the day. Ten of 40 people left their cards in the reader overnight and 6 people left their cards home. No one reported losing their card and no cards were reported stolen. During interviews, participants said that they were concerned about the fact that their "other" ID card – the original card that granted only physical access – was slated for deactivation. As long as the username/password can be used to access computers, forgetting a PIV card is not likely to impact productivity (unless users forget their passwords due to disuse).

On the other hand, lost or stolen cards can cause serious problems, not least of which is a 7-14 day period for replacement. Participants were acutely aware that a lost PIV card meant lost PKI certificates: because the certificates were on the card and nowhere else, anything encrypted with a lost card would be unrecoverable. It is not surprising that many users expressed hesitancy to use encryption since a lost certificate would prevent them from accessing the material. Their concerns over the potential loss of certificates and encrypted material discouraged them from using the encryption functionality of the card for any information they might need to retrieve later.

5.3.2 Windows 7 card support compared with XP implementation using ActivClient

During the usability pilot, a few users upgraded to Windows 7, giving us the opportunity to see the operating system's PIV interface and watch users interacting with the system. PIV interaction using Windows 7 is very different from that seen in ActivClient middleware on a Windows XP system. The problem from a user's point of view is that anything learned with one system will not help when using the other system. Similarly, users may perceive benefits with one system that aren't available with the other. For example, with ActivClient and XP card removal results in screen locking; users highlighted this as a key benefit of smartcards. Windows 7 does not offer this interaction as the default. Another example is that ActivClient detects when a card is inserted and responds by showing a PIN dialog; Windows 7 always asks the user to say whether he or she would like to use the PIV/PIN[17] or the username/password, adding one extra level of dialog to each unlocking of the screen. Differences between the ActivClient and Windows 7 PIV interfaces meant that users who upgraded to the latter faced additional challenges in adjusting to the daily use of smartcards.

5.3.3 PIN vs. Password

As the password policy has become more onerous, our participants found use of a 6-8 number PIN a significant benefit of using smartcards. It was easy to remember, easy to perform error-free entry and did not need to be changed. The only down-side to routine PIN use was that it was more difficult for users to remember their passwords. In interviews, some participants reported that the only time they needed to know their password was to maintain/change their password. While passwords can be a useful fallback for users who cannot use their smartcard for some reason (e.g., they misplaced it), there is a significant possibility that they may forget their password due to disuse. In the event that they *don't* ever need to fall back on their passwords, users may find the necessity of changing it on a regular basis to be frustrating.

5.3.4 Limited number of Web applications support PIV authentication

We found that users who currently use web applications as a core part of their workflow (e.g., NAIS) appreciated the ease of using PIV cards for accessing these applications. During interviews and in the final survey given to all pilot users, we solicited users' ideas about other applications that they would like to see with PIV authentication. Most users in the survey said "all of them!" Specific examples they gave include: HR and Budget apps, ACS,

[17] And, technically, PKI certificates – but those are "invisible" to the user most of the time.

PPS, CBS, CLC, CSAM, NNIS, C.Request, TravelManger, E-Approval, EPP, Remedy, WebTA, BizFlow, Toad, Citrix, CSTARS.

5.3.5 Guidance on when to encrypt or digitally sign documents/messages

Users learned to encrypt and sign messages and documents with their smartcards. Some participants explored using encryption to send passwords to users; others shared PII and financial information with group members. Nearly all participants used digital signatures to test whether they could make it work. During the course of the usability pilot, NIST released a policy directive saying that PII could only be sent via e-mail if the e-mail was encrypted. Users told us during interviews that they were glad to have a policy to guide their use of PII in their workflow. There was, however, no similar recommendation for when a digital signature should be used. There was likewise no guidance for the recipient of a digitally signed e-mail to help in understanding what value to assign to a digital signature. Our participants were exceptionally willing to follow policy; they were, however, reluctant to make up a personal policy regarding PIV use in the absence of any organizational guidance.

5.3.6 Guidance on selecting the correct digital certificates

All study participants had at least three digital certificates on their smartcards. In certain situations during the course of PIV card use (e.g., using the web application for registering visitors), dialogs appeared that required the user to select a certificate to apply. The content of the dialogs was dependent on the browser; Firefox seemed marginally more comprehensible than IE7.[18] These dialogs did not provide any guidance to users on how to choose the "correct" certificate for the situation. Most users just selected the highlighted default. The fact that the underlying Web app would accept either certificate gave the user a sense of having chosen correctly, but in truth either selection would have worked: one simply required the user to enter a PIN and the other would not require a PIN. There was no way for the user to learn from the situation. If anything, they learned to close their eyes and choose.

5.3.7 Using PIV while working on multiple computers

Quite a few technical users needed to be logged into more than one computer in their workspace at a time. Some configurations used VPN and others used separate physical computers. The users of these systems were always quite technically capable. They learned

[18] The appearance of dialogs asking the user to select a certificate – and the fact that these dialogs differed depending on the browser – were unanticipanted issues, and therefore were not addressed in the "Test Scenarios and Instructions" document described in **Section 5.1.3**.

optimal ways of accessing computer resources and discovered best practices for using PIV when possible.

5.3.8 Dealing with critical system failures (e.g., driver error that causes a system to keep rebooting)

The usability team found that people attribute any computer problem to the last thing that was changed on their computer. This heuristic has been learned and reinforced through long experience with using computers. In one sense, this mental model is good at detecting real problems especially ones that are severe. For example, when users called for help with a hardware driver error that caused their system to malfunction, they correctly attributed the cause to the middleware for their PIV readers. On the other hand, subtle issues like resetting the domain or resetting the default for digital signatures were not so serious. People could still get work done but both issues were frustrating since solutions were not apparent to the user. Given how much remote administration goes on in large and/or geographically dispersed locations, users in these environments are used to defaults changing and to items being reset to different values; this makes it hard for the user to know whether a change has been made "on purpose" or whether it might actually be a reportable problem.

5.4 OVERALL ACCEPTANCE

5.4.1 Users develop inaccurate mental models of security

We asked the usability participants whether they believed that the PIV/PIN combination is more secure than the username/password combination. Some participants agreed that it was **(**Table 2). However, when we asked these participants to tell us *why* PIV/PIN is more secure, only seven provided an answer indicating that they understood why 2-factor authentication is more secure. Many other participants said that they didn't know if the PIV/PIN combination was more secure. A few believed that guessing a short, numeric PIN would actually be easier than guessing a long, complicated password – forgetting that possessing the card (and by extension necessary PKI credentials) is part of the overall scheme and provides an additional layer of security. This can probably be attributed to the fact that, while these users may have had a reasonably good idea of how passwords work, they were completely unfamiliar with multi-factor authentication.

While educating users about security may help increase security, users will never be security experts, nor should they be. If new or additional security measures do not have an obvious benefit to users, it will be difficult for them to adopt the new technology or process.

5.4.2 Users who interacted with the usability team adopted the smartcards more readily than others

There is little reason to suspect that the participants from the OCIO pilot who volunteered for the usability sub-study were different from those who didn't. The characteristics of the groups are similar with respect to age, job title, career path, and education. There are, however, some differences between the groups with respect to perceptions and attitudes. The most salient of these are that users in the usability pilot: 1) used their PIV cards more during the pilot (Table 2); and 2) say they are much more likely to continue using their PIV cards for accessing their computers (Table 6).

It is not possible to state with any scientific certainty what caused participants who interacted with the usability team to enthusiastically adopt smartcards. However, it is reasonable to suggest that incorporating some of the methods employed by user-centered practitioners could help in future efforts to encourage good security behavior. The members of the usability team were sympathetic when users complained, were patient while users described problems they were experiencing, and were helpful when help was requested; they reminded people that there was documentation that they could read and that there were knowledgeable people they could call for help. Most of the interaction between a user and a usability team member was a matter of encouraging the user to take charge of his own PIV experience.

6. CONCLUSIONS AND FUTURE WORK

As previously stated, the purpose of this pilot study was to understand the factors that affect user behavior and perceptions in the use of smartcards for authentication and to examine factors that affect user behavior and perceptions of security.

Exploring this issue provided us with some insights into how organizations can reduce the drawbacks and maximize the benefits of smartcards for their user population. In general, security must be as transparent as possible and maximize direct benefits to users. It should make minimal demands on users' time and effort, and interfere as little as possible with their primary jobs. Transparent and minimally burdensome security technologies and rules make it easier for users to practice good security behavior.

For example, organizations that adopt PIV cards should preserve one of the greatest perceived benefits of smartcard PINs over passwords: that the PIN does not need to be changed frequently, the way passwords do. From a usability perspective, once a user creates a PIN, they should be able to keep it for as long as they keep their smartcard (only when the smartcard must be replaced should the PIN be changed). If possible, the PIV cards should be part of an organizational SSO solution (or some form of login consolidation): while SSO is

difficult to implement, it has considerable appeal from a usability perspective, and may make users more enthusiastic about adopting PIV. Finally, usernames and passwords should still be available to users in the event that they cannot use their smartcard.

It is also necessary for organizations to try to get it right the first time where smartcard initialization is concerned – or, at the very least, to be able to resolve any initialization errors quickly and with minimal inconvenience to users. Our study participants' problems with updating their PIV certificates underscores the critical importance of a streamlined certificate update process. The software needs to work correctly, the responsible personnel need adequate training and support, and cards should be tested immediately after any update to ensure that they will function properly. Ideally, organizations should automate the process as much as possible, which would make it easier for them to provide employees with walk-up update services near their workplace (e.g., using a kiosk or the appropriate features in some smartcard middleware).

On a related note, any organization that issues PIV cards should be able to replace lost or stolen cards as soon as possible. The organization should also have a (secure) way to recover/maintain digital certificates and keys associated with PIV cards so that any information encrypted with a card that is subsequently lost, stolen, or broken can be recovered (e.g., via key escrow). In addition, the organization should develop a strategy for coordinating technical support for users of PIV cards and readers: technical personnel should know how to resolve any common problems or, at least, be able to escalate any user issues to the appropriate party, whether that be a PIV system support technician or the manager of the user's organizational unit (or, in some cases, both).

Technical support personnel who are responsible for installing PIV readers should be prepared to act in the capacity of a short-term trainer and coach. PIV cards are a relatively new development and many users (though certainly not all) will need someone to answer their questions about the system and provide them with a hands-on demonstration of how to use the card and reader. Installation personnel should also be able to direct users to appropriate resources – such as training videos or documents – to which they can refer for additional information on PIV use. Generally speaking, a variety of informational/training resources related to PIV (e.g., brochure, video, website, instructor-led course) should be available to users in order to accommodate their varying learning styles and preferences.

One way to help provide informal learning opportunities for users and foster acceptance of the PIV system is to initially pilot the use of PIV cards among self-selected users from a cross-section of the organization (i.e., from different departments and functional areas). When the PIV cards are later rolled out to a wider audience, some of these early adopters may be able and willing to help new users make a smoother transition to using the PIV

system. Piloting the PIV system with a diverse user group will also allow the organization to discover and remediate any problems prior to large-scale implementation.

In addition to training users in the simple logistics of using a PIV card to log into/out of a computer and authenticate to applications, organizations should provide their users with guidance on when to employ digital signatures and/or encryption. This guidance should combine both organizational policy and rationale. It should also be as easy as possible for users to choose the correct digital certificate for a particular purpose (e.g., digital signing, encryption). Ideally, that process should be automated if possible. If that is not possible, it should at least be easy for users to distinguish between certificates when prompted for a choice: Windows 7 can be configured to list digital certificates by descriptive names (e.g., "Authentication Certificate," "Encryption Certificate"). However, this solution can only be implemented on an individual basis. The policies, processes, and mechanisms associated with digital certificate use should be worked out before organization-wide implementation of a PIV system.

The timing of large-scale PIV implementation in relation to other IT system changes or overhauls is also important to consider. If an organization is considering changing the operating system on end users' workstations, for example, the organization should wait until this change has gone through (and give users adequate time to adapt to the new OS) before issuing PIV card readers. This is because the behavior of the PIV interface may change depending on the OS, and user behaviors and habits learned on one interface will not transfer to another.

Finally, when organizational users are issued their PIV cards, they should also be given the option to choose from a variety of reader devices, according to their needs. Based on our usability pilot, built-in laptop readers seem to be the most convenient for users (and many laptops now come standard with integrated readers), but that is not always an option. Some kind of USB reader that can clip to a monitor might be the best solution for those who cannot use laptop or keyboard readers: such a device would remove the need for two-handed operation and solve the "out of sight, out of mind" problem that some participants had with their USB readers. Another possible option is to use a reader that can detect the user at a distance (e.g., with BlueTooth[19]), but such devices are not common and may be harder to secure. While the cost of readers is important to consider, the possibility that organizational

[19] There is a type of BlueTooth-enabled smartcard holder that can read the PIV card it contains and communicate via BlueTooth to a PC or other paired device.

units or individuals may be willing to pay more for increased convenience should be factored into any decision as well.

While more work remains to be done in the area of PIV usability, the findings of our study highlight one fundamental fact: most end users do not understand the organizational security benefits provided by PIV systems, but they *do* understand the usability benefits – provided the PIV system and associated organizational mechanisms are designed with usability in mind. In the short term, a usability-oriented PIV system will help ease users' adaptation to using that system, in part by making them more willing to embrace it. In the long term, it will help the organization realize the fullest possible return on its investment in the system.

7. REFERENCES

[1] Arora, S.: National e-ID card schemes: A European overview. Information Security Technical Report, 13(2), 46-53 (2008).

[2] Baldwin, M.K. and Malone, B.M.: Utilizing Smart Cards for Authentication and Compliance Tracking in a Diabetes Case Management System. In proceedings of ACM Conference on Software Engineering, 521-522 (2008).

[3] Braz, C. and Robert, J.M.: Security and Usability: The Case of the User Authentication Methods. In proceedings of d'Interaction Homme-Machine, 199-203 (2006).

[4] Identity, Credential and Access Management Subcommittee.: The Realized Value of the Federal Public Key Infrastructure (FPKI) v1.0.0. January 29, 2010 (2010). http://www.idmanagement.gov/

[5] Irwin, C.S. and Taylor, D.C.: Identity, Credential, and Access Management at NASA, from Zachman to Attributes. In proceedings of IDtrust 2009, 1-14 (2009).

[6] Karger, P.A.: Privacy and Security Threat Analysis of the Federal Employee Personal Identity Verification (PIV) Program. In proceedings of the Symposium on Usable Privacy and Security 2006, 114-121 (2006).

[7] Landsberger, H. A. (1958). Hawthorne revisited: Management and the worker, its critics, and developments in human relations in industry. Ithaca, NY: Cornell University.

[8] Muller, M. J. and Kogan, S.: Grounded Theory Method in HCI and CSCW. IBM technical report 10-09 (2010). http://domino.watson.ibm.com/cambridge/research.nsf/58bac2a2a6b05a1285256b30005b3953/818eb1454a54b9348525777d0071c35c!OpenDocument

[9] Murdoch, S.J., Drimer, S., Anderson, R., and Bond, M.: Chip and PIN is Broken. In proceedings of IEEE Symposium on Security & Privacy 2010, 433-446 (2010).

[10] National Institute of Standards and Technology: Personal identity verification (PIV) for federal employees and contractors. FIPS PUB 201-1 (2006).

[11] National Institute of Standards and Technology: A Scheme for PIV Visual Card Topography. NIST SP 800-104 (2007).

[12] Office of Management and Budget, Office of E-Government & Information Technology: Q4 FY11 – HSPD-12 public report summary (2011). Retrieved from: http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/hspd-12_publicreportsummary-q4fy2011.pdf

[13] Proctor, R.W., Lien, M.C., Salvendy, G., and Schultz, E.E.: A Task Analysis of Usability in Third-Party Authentication. Information Security Bulletin, 5(3), 49-56 (2000).

[14] Sasse, M.A.: Usability and Trust in Information Systems. Cyber Trust & Crime Prevention Project. University College London (2004).

[15] Strouble, D.D., Schechtman, G.M., and Alsop, A.S.: Productivity and Usability Effects of Using a Two-Factor Security System. In proceedings of SAIS, 196-201 (2009).

[16] U.S. Department of Homeland Security: Policy for a common identification standard for federal employees and contractors. Homeland Security Presidential Directive HSPD-12. August 27, 2004 (2004).

[17] U.S. Department of State: Biometric Security Vulnerabilities and DoS Defenses v1.0, June 2010 (2010). Point of contact, Steven Gregory <gregoryse@state.gov>

[18] U.S. Department of State: Cost/Benefit Comparison between PKI/BLADE and Password-Based Authentication v1.0, July 2010 (2010). Point of contact, Steven Gregory <gregoryse@state.gov>

APPENDIX A: PARTICIPANT SURVEYS

The following items are the full versions of surveys employed by the usability research team to collect feedback from participants. These include: the daily e-mail survey; the Pre-Installation and Post-Installation surveys; the periodic Card Use survey; and the Exit survey.

A.1 DAILY E-MAIL SURVEY

About Accessing your computer				
	Yes	*No*	*If 'yes',*	
1. Did you use **PIV to log in** today?			Describe any positive aspects:	Describe any negative aspects:
2. Did you **stop using PIV** at any point today?			Why?	
3. Did you **use your username and password** to log into the NIST network today?			Why?	

About Encryption and Digital Signatures			
	Number	*If you used the feature,*	
4. How many **encrypted emails** did you send today?		Describe any positive aspects:	Describe any negative aspects:
5. How many **digital signatures** did you apply today?		Describe any positive aspects:	Describe any negative aspects:

About Registering Visitors			
	Number	*If you used the feature,*	
6. Did you use your PIV PIN to register any visitors today?		Describe any positive aspects:	Describe any negative aspects:

Miscellaneous			
	Yes	*No*	*If 'yes', why?*
7. Did you call iTAC today about PIV use?			

Comments [use as much space as you want to tell the usability team about anything not covered in the rest of the survey]

A.2 PERIODIC SURVEYS

These questionnaires were administered to participants at different points in the survey (as indicated by the titles preceding each).

A.2.1 Pre-Install Survey

Pre-installation questionnaire [ID:_____ Date: _____]

Before you start using the PIV authentication system, please rate your responses to the following statements:

1. I'm confident I know how the new authentication system works and what it will do.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

Do you have any questions about the new authentication system? If so, list them here.

_____

_____

_____

2. I am confident that I know how to encrypt an email using the PIV card.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

Do you have any questions about the email encryption process? If so, list them here.

_____

_____

3. I am confident that I know how to digitally sign a document/email using the PIV card.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

Do you have any questions about the digital signature process? If so, list them here.

4. I am confident that I know how to register a visitor to NIST using the PIV card.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

Do you have any questions about using PIV for the visitor registration process? If so, list them here.

5. Compared to using passwords, using the PIV will be more secure.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

Why or why not?

6. The new PIV authentication system will make the log-in process **easier** than the current password based log-in systems.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

7. The new PIV authentication system will make the log-in process **faster** than the current password based log-in systems.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

8. Using the PIN for the PIV card will be easier than using a password.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

9. I'm looking forward to using this new authentication system.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

10. I plan to use the new authentication system routinely.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

11. I plan to continue using my password instead of the PIV when logging in.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

12. I received the training document ("PIV Pilot Test Scenarios and Instructions") from Aiping? [Yes/No] _____

13. If you received the document, did you read it? [Yes/No] _____

14. Did you print it? [Yes/No] _____

15. Do you have any concerns or questions before you start using it?

_____

_____

_____

_____

A.2.2 Post-Install Survey

Questionnaire: [ID:_____ Date: _____]

1. I'm confident I know how the new authentication system works and what it does.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

Do you have any questions about the new authentication system? If so, list them here

_____

_____

_____

_____

2. The training document ("PIV Pilot Test Scenarios and Instructions") provided a clear understanding of how to use the new authentication system.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

What would you suggest to improve the training you received?

_____

_____

_____

3. The new authentication system makes the log-in process easier than the current password based log-in systems.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

4. The new authentication system makes the log-in process faster than the current password based log-in systems.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

5. I plan to continue using my password instead of the PIV when logging in.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

6. Using the PIN for the PIV card is easier than using a password.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

7. I plan to use the new authentication system routinely.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

8. Can you envision any occasions when you would be unlikely to use the PIV but would instead want to use your password? If so, describe those situations.

9. What other applications and benefits do you see in using the PIV system?

A.2.3 Card Use Survey

1. I am confident that I know how the new authentication system works and what it does.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

Do you have any questions about the new authentication system? If so, list them here

2. I am confident that I know how to encrypt an email using the PIV card.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

Do you have any questions about the email encryption process?

3. I am confident that I know how to digitally sign a document/email using the PIV card.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

Do you have any questions about digital signature process?

4. The new authentication system makes the log-in process easier than the current password based log-in systems.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

5. The new authentication system makes the log-in process faster than the current password based log-in systems.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

6. I will continue using my password instead of the PIV when logging in.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

7. Using the PIN for the PIV card is easier than using a password.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

8. I take the PIV card with me every time I leave my computer.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

9. I plan to use the new authentication system routinely.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

10. I would encourage my colleagues to switch to the PIV authentication system.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

A.2.4 Exit Survey

PIV Usability Study Exit Survey

1) I am confident that I know how the new authentication system works and what it does.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

2) The new authentication system makes the log-in process easier **than the current password based log-in systems**

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

3) The new authentication system makes the log-in process faster **than the current password based log-in systems**

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

4) The new authentication system is more secure **than the current password based log-in systems**

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

5) Using the PIN for the PIV card is easier than using a password

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

6) I plan to continue using my password instead of the PIV when logging in

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

7) I take the PIV card with me every time I leave my computer

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

8) I have enjoyed using the new authentication system

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

9) I plan to continue to use the new authentication system after the conclusion of this study

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

10) I would encourage my colleagues to switch to the PIV authentication system

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

11) If you have any comments, questions, or feedback about the PIV authentication system, please list them here

12) If you have any comments, questions, or feedback about the PIV Usability Study, please list them here