A Field Study of User Behavior and Perceptions in Smartcard Authentication

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

A Field Study of User Behavior and Perceptions in Smartcard Authentication

Celeste Lyn Paul[1], Emile Morse[2], Aiping Zhang[2], Yee-Yin Choong[2], Mary Theofanos[2]

[1] University of Maryland Baltimore County
1000 Hilltop Circle, Baltimore, Maryland, United States
cpaul2@umbc.edu

[2] National Institute of Standards and Technology
100 Bureau Drive, Gaithersburg, Maryland, United States
{emile.morse, aiping.zhang, yee-yin.choong, mary.theofanos}@nist.gov

Abstract. A field study of 24 participants over 10 weeks explored user behavior and perceptions in a smartcard authentication system. Ethnographic methods used to collect data included diaries, surveys, interviews, and field observations. We observed a number of issues users experienced while they integrated smartcards 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 in replacement of complicated passwords. The greatest perceived drawback was the lack of smartcard-supported applications. Overall, most participants had a positive experience using smartcards for authentication. Perceptions were influenced by personal benefits experienced by participants rather than an increase in security.

Keywords: Human factors, multi-factor authentication, security, smartcard

1 Introduction

In an attempt to protect their valuable data, organizations such as banking and financial institutions, corporations, and governments spend a large fraction of their information technology budgets on security [9]. Because of security, users of these systems must adhere to new business rules, information security policies, and training sessions – which takes time and effort away from their primary jobs.

There is a constant tension between users who are trying to get work done and security specialists who lock down systems to make them safer and more secure. Despite not being the security specialists, the burden of maintaining a secure work environment often falls on users. While the efficacy of such security practices can be debated [7], it is clear that there is a role for HCI researchers to play in understanding

how users and security can be optimized to serve both. Users have often been described as the “weakest link” in information security, but they lack the proper motivation and tools to effectively contribute to the information security ecosystem [18]. Many approaches designed to increase security have placed additional burdens on users. Users now have longer, more complex, and more frequently changing passwords [23]; more restrictions on what they can do on the web [20], and they must use additional keys, tokens, or cards in order access information systems [2].

Homeland Security Presidential Directive 12 (HSPD12) [24] defines requirements for a standardized, U.S. Government-wide identification mechanism for a reliable identification credential. Personal Identity Verification (PIV) [15] is a smartcard-based multi-factor authentication (MFA) mechanism to increase security of government resources. The PIV smartcard contains personally identifiable information (PII) about the card holder such as his full name and agency, PKI certificates for authentication, encryption, and digital signature, and biometrics such as fingerprints and photo. It can be used for physical building access, for information system authentication, to support PKI, and as an identity card.

The PIV smartcard affects hundreds of thousands of U.S. Government employees and contractors. While the use of the smartcard is mandated by policy, we are concerned with how introducing 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, e.g. weekly use of an Automatic Teller Machine (ATM) card. This is one of several reasons why we studied user behavior and perceptions using smartcards.

1.1 Research Goals

The purpose of this 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 had three main goals for the study. First, we wanted to learn how users would use the smartcards in their everyday work processes. Second, we wanted to learn how users' work processes might change to accommodate smartcard use. Third, we were interested in the user benefits and drawbacks of using smartcards in authentication.

2 Related Work

Multi-factor authentication (MFA) is the use of two or more independent security factors to authenticate to an information system. There are three factors commonly used in MFA [16]. The first factor is “something you know” such as a password, passphrase, or personal identification number (PIN). While passwords are perhaps the

most common “something you know” authentication factor, challenges to password usability include the cognitive limits related to the number of passwords [6] and length of passwords [23] users must remember. A second factor is “something you are”, i.e. using biometrics such as fingerprints or a facial image. A benefit of using a biometric as an authentication factor is that it does not depend on secrecy [16]. It is something users will always have with them and will never need to remember. The third factor is “something you have” such as a key, token, or card. ATMs are a classic example of MFA using a card in combination with a PIN [26]. There are also additional authentication factors not as commonly used. For example, “someone you know” considers social network characteristics such as who you went to school with [4, 21]. Another factor, “something you do” considers behavioral characteristics such as online shopping habits [12].

In this paper, we focus on the “something you have” authentication factor, specifically the use of smartcards in MFA. Smartcards are tokens that include embedded chips that can store information. Smartcards are different from magnetic strip cards in that while both can store data, the chip in smartcards makes them more secure and provides more features. A smartcard can be used for MFA in several ways. The smartcard can be “something you have” by acting as a token. It can be used along with “something you know” such as a password or PIN. Smartcards can also support the “something you are” factor by storing biometric data on the embedded chip that can later be matched to the user.

Examples of smartcards used as authentication tokens similar to PIV include the European national electronic identity (e-ID) card [1] that stores different types of PII depending on the requirements of the issuing country. The U.S. Department of State uses the Biometric Logical Access Development and Execution (PKI/BLADE) card as an employee identity card and authentication token [8, 25]. The U.S. Department of Defense uses the Common Access Card as a military identity card, Geneva Conventions Identification Card, and authentication token [8].

While work has focused on smartcard security weaknesses such as problems with the embedded chip and PIN mechanism [14] and PIV implementation standard [11, 13], very little work has looked at smartcard usability [19]. Proctor et al. [17] 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 [5] 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 [3] described the use of smartcards in a health management system. The ability to store information, such as PII, 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 PIN on their userbase [25]. 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. 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. [22] conducted a survey that looked at issues concerning security, usability, and productivity of smartcards. They found the use of a PIN 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 Methodology

3.1 Participants

We studied 24 participants from a U.S. Government research institute over a period of approximately 10 weeks. There were 10 males, an average age of 47 (SEM ± 2), and and a distribution of education that was representative of the organization (8 high school degrees; 10 college degrees; 6 post-graduate degrees). Ten participants were engaged in technical work; five were support staff, e.g. secretarial work; and nine worked in an administrative specialty, e.g. finance. Two participants reported having experience with smartcards before the study.

Our study participants were recruited from an institution-wide technology pilot of 100 users testing the PIV smartcard technology. The technology pilot used the same smartcard system as our study; the only difference was that our study included additional research methodologies to assess the smartcard system. Recruitment in the technology pilot was designed to include test users from a representative sample of users in the institution, except for research scientists. Even without scientists, the technology pilot had a sampling of job roles and education similar to an industry corporation. Our study sample reflected the same demographics as the overall groups recruited in the technology pilot; except in our study there was a higher proportion of females. Participation in both the technology pilot and our study was voluntary. However, all participants were aware that the smartcard system would soon be mandatory for all users.

Fig. 1. From left to right: USB reader, laptop reader, integrated keyboard reader

3.2 Study Environment

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. Participants had both an identity card and a smartcard. Participants also had both smartcards/PINs and usernames/passwords. The smartcard PINs were 6 to 8 numbers long and selected by participants at the time of smartcard issuance. The password length policy was 10 characters at the beginning of the study and changed to 12 characters one week after the study began. Passwords expired every 90 days and every participant changed passwords at least once during the study. Participants used their own computers and workspaces. Participants used either a laptop or desktop computer. 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. All computers were running Windows XP with ActivClient smartcard middleware[1]. One of three types of smartcard readers was used by each participant (Fig. 1): an external USB reader (n=13), an internal laptop reader (n=6), or an integrated keyboard reader (n=5). 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 email or document, and authenticate to several smartcard-enabled web applications. In each case, participants could authenticate with either their smartcards/PINs or usernames/passwords.

3.3 Data Collection Methods

Several ethnographic research methods were used to obtain a breadth of coverage as well as a depth of understanding of our participants over the course of the study.

1 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.

Table 1: Summary of study phases and data collection methods

Installation		**Smartcard Use**			**Wrap-up**
Pre-Install	*Post-Install*	*Daily*	*2-Week*	*6-Week*	*Exit*
Survey	Site visit Interview Survey	Daily diary Daily email	Site visit Interview Survey	Site visit Interview Survey	Site visit Interview Survey

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.

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

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 were also given space for several questions to provide additional comments. 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.

Daily Diaries. Participants were asked to keep daily written diaries of notable smartcard events. We provided notebooks for them to write in and a guide on the types of events to note, such as forgetting to login using the smartcard. If participants were not comfortable writing in the provided notebook, they were encouraged to keep notes in an electronic document.

Daily Email Surveys. The daily email 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 email surveys was to supplement the daily diaries as a way of reporting critical events, and not as a quantitatively evaluated questionnaire.

Site Visits and Interviews. Site visits allowed us to observe smartcard use in the participant's natural environment. Interviews provided an opportunity to discuss participant's smartcard experience since the previous visit and review any critical events that were reported in the daily diaries or daily email surveys. Field notes from the site visit observations and interviews were recorded.

3.4 Procedure

The study was conducted in three phases: Smartcard Installation, Smartcard Use, and Study Wrap-Up. See Table 1 for a summary of research activities.

Smartcard Installation. Before we met with participants, we sent the Pre-Install survey and a technical support person provided a brief training document via email. Participants were asked to complete the Pre-Install survey before the first site visit. The training document contained a step-by-step scenario guide on how to complete smartcard-related activities. The technical support person then installed the smartcard hardware and software, demonstrated how to use the smartcard, and guided participants through several smartcard use scenarios. The support person also asked participants to perform tasks, such as locking and unlocking their computers. After installation was complete, we conducted the Post-Install site visit. We observed participants using their smartcards, interviewed them about their first time experiences with the smartcards, administered the Post-Install surveys, and provided them the Daily Diaries and guide.

Smartcard Use. During smartcard use, participants were asked to keep diaries of notable smartcard usage and events. The daily email survey was sent near the end of the day for participants to complete and return. Researchers would review the daily diaries and email 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 the researchers observed participants using their smartcards, interviewed them about their smartcard experiences to date, and administered the 2-week or 6-week surveys.

Study Wrap-up. Study wrap-up activities took place between 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.

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

Periodic Survey Statement				
Pre-Install	*Post-Install*	*2-Week*	*6-Week*	*Exit*
1. User confidence with smartcard				
3.50 ± 0.38	4.42 ± 0.19	4.33 ± 0.30	4.12 ± 0.40	4.20 ± 0.34
2. Remembering smartcard				
–	–	3.67 ± 0.47	4.04 ± 0.43	3.88 ± 0.41
3. PIN is easier than password				
3.5 ± 0.29	3.92 ± 0.38	4.17 ± 0.28	4.24 ± 0.38	4.32 ± 0.39
4. Smartcard easier than password				
3.40 ± 0.34	3.73 ± 0.39	4.08 ± 0.35	4.24 ± 0.31	4.24 ± 0.31
5. Smartcard faster than password				
3.33 ± 0.33	3.50 ± 0.41	3.83 ± 0.40	3.68 ± 0.52	3.64 ± 0.49
6. Smartcard more secure than password				
3.73 ± 0.34	–	–	3.60 ± 0.32	3.84 ± 0.29
7. Smartcard adoption				
4.19 ± 0.19	4.35 ± 0.19	4.29 ± 0.38	–	4.48 ± 0.32
8. Recommend smartcard to colleagues				
–	–	4.08 ± 0.33	4.04 ± 0.26	4.32 ± 0.31
9. Smartcard satisfaction				
3.92 ± 0.26	–	–	–	4.32 ± 0.29

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 reflect on the methodology and provide lessons learned.

4.1 Descriptive Statistics of Quantitative Methods

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.

Daily Email Surveys. There were a total of 682 daily email surveys collected; the average number of emails collected from each participant during the study for each

participant was 28.4 (SEM ±2.5). The number of email 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 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.

4.2 Analysis of Observations

Table 3 provides a summary of reported issues with discussion in the following section.

User Confidence. Participant confidence in using the new smartcard authentication system increased immediately after installation (Pre-install/Post-install: W=3.87, p=0.001) and remained high throughout the study (Post-install/Exit: Kendall's W=0.04, p=0.41).

Seventeen 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 attended training. 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).

Smartcard Readers. Fifteen participants used USB readers that were placed on their desks. 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 blamed his USB reader for why he forgot 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 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, an additional problem with the USB reader was that it was not attached to a stable object and required participants to use two hands when

Table 3: Summary of study observations by issue topic.

Issue Topic	Observation
User Confidence	• Confidence in using smartcards increased after Installation
Smartcard Reader	• 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 otherwise • Unattended smartcard message is sometimes useful
Password vs. PIN	• 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

removing and inserting the smartcard. One participant remedied this problem by attaching her USB reader to her computer with rubber bands.

Not all participants could use a keyboard reader because their keyboards were in keyboard trays attached to their desks. Several of these participants who used keyboard trays also kept their keyboards partially hidden under their desks while they typed. Unless the keyboard was completely pulled from under the desk, it would not fit under the desk with the smartcard in the keyboard reader.

Using Smartcards. Remembering to remove their smartcards from their readers was a commonly reported incident by participants. Thirteen participants (54%) forgot their smartcards in their readers at least once during the study. The most common scenario for participants to forget their smartcards was during short trips out of their work

areas, such as down the hall to visit a colleague or visit the restroom. Three 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 of 24 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 login. 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 for 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 login or lock 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 login 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. The design of the login dialog may have contributed to whether participants used their usernames and passwords to login. By default, the computer displayed a username and password dialog instead of a PIN dialog. A few participants discovered if they pressed Escape on the keyboard with their smartcards in their readers, a PIN dialog would display. This information was shared with the other participants. If participants did not use the smartcard to login to a session, they would not be able to remove the smartcard from the reader in order to quickly lock the computer. This caused some confusion in the beginning of the study when participants were not yet consistently using the smartcard to login, “*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.

Participants were neutral whether smartcard authentication was faster than passwords (Exit: 3.64 ± 0.49). Nine participants noticed that using smartcards took longer to authenticate and login than using usernames and passwords. Smartcard login was observed by participants to take 10-30 seconds longer than their password logins. 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 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).

Passwords vs. PINs. Overall, participants found using the smartcard easier than using passwords (Exit, 4.24 ± 0.31). Participants also found that logging in with the PIN was easier than using their passwords (Exit, 4.32 ± 0.39). 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. The PIN never expired compared to the system password that expired every 90 days. The PIN was six to eight characters in length compared to the system password requirements of 10 or 12 characters in length. 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 how the new 12-character password requirement 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 before the study. Several participants felt they were at risk for forgetting their passwords, "*It is an effort remembering my system password*" (P15). Some participants needed their primary network password to login to computers that were not smartcard-enabled, providing an opportunity to practice their passwords if they were synced. However, participants who did not sync passwords or used their passwords to only login to their computers were at a greater risk for forgetting.

Participants also described various ways they managed passwords before their experience with smartcards. Nine 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 syncing passwords 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 sync. It was also a hassle to retrieve a password for every account. Two participants reported using software to save and manage passwords. Some participants anticipated the smartcard moving towards a SSO solution, "*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).

Certificates. Authentication was supported for several web applications. Participants authenticated to web applications by visiting the login page. 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 choose. If participants chose the non-repudiation certificate used for digital signatures, they were asked to enter a PIN. If participants chose the certificate used for encryption, they were not asked to enter a PIN. However, without expert knowledge in certificates it was difficult for participants to identify the encryption certificate from the digital signature certificate.

The smartcard authentication system also does not allow certificates to be backed up or saved/transferred. Three participants expressed concerns about the lifetime of certificates used to encrypt email and documents. If a smartcard is lost, stolen, expires, or is replaced, the certificates are lost forever. Previously encrypted email and documents could no longer be decrypted and the information would no longer be accessible. One of the participants worked with financial information and was concerned with not being able to access old encrypted data because his data needs to be available for auditing.

Digital Signatures and Encryption. The most infrequently used smartcard features were digital signatures and encryption. Once familiar with the functionality, participants were comfortable with digitally signing and encrypting email and documents and found both easy to use. However, most participants did not know when they would have a need to sign or encrypt an email 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 email or documents; although, several participants routinely tested the features. Several participants stated they would not consider using signing and encrypting unless it became policy, "*I see no value in a digitally signed email and would do so only if I was required to*" (P23). Two participants tried encryption to send passwords through email, 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.

All participants unintentionally signed email at some point in the study due to a technical problem that temporarily changed an option in their email clients. While most participants immediately noticed a difference in behavior and found typing a PIN for every sent email inconvenient, one participant decided to experiment with email 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 the functionality might not be for everyone, "*I send a small number of emails 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. As one participant expressed his doubts about the usefulness of digital signatures, "*I don't see the point. People are going to know who I am based on what I say in the email*" (P2).

Participants who worked regularly with PII considered the possibility of signing and encrypting email or documents, but in practice found it impossible to use with the current smartcard implementation. PII in the workplace was shared between coworkers 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 were setup and supported for sharing.

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 described, "*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. There were 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. 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).

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 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, she did not consider this when she developed this behavior.

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 3 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 (Exit, 4.48 ± 0.32). 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 login*" (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 Methodology Lessons

This study utilized a number of qualitative field methods including daily diaries, daily surveys, periodic surveys, periodic user interviews, and field observations. The lessons learned in this study will help improve the design and methods of future work.

Most participants kept the written diary until the 2-week interview, but few participants wrote much after that. Several participants kept a written journal in a text file on their computers because they felt it was easier to keep than a written diary. Most participants summarized daily diary events in the daily surveys. Despite the lack of participation in keeping the daily diaries, we feel that providing the diaries helped participants understand the purpose and type of information we were interested in. Although the study designs were different, our methodology experiences are consistent with those reported in a diary study of password use conducted by Inglesant and Sasse [10].

As previously discussed, daily surveys were answered more frequently by participants in the beginning of the study than at the end of the study. When asked during interviews, several participants reported not responding to daily surveys because they did not have new events or comments to report and felt their responses would not add value to their participation. Modifying daily survey questions to fit with participants' evolving user experience could help encourage continued daily survey participation.

We observed participants' smartcard use from installation through 10 weeks of use. We observed new behaviors and perceptions up to six weeks after installation. After six weeks up until 10 weeks of observation, the rate of new observations was infrequent. At a minimum, we recommend users be studied for six weeks to be able to observe any transitions from learning to everyday use. Observations for less than two weeks after installation would not be sufficient to fully understand the impact the new technology has on participant behavior and perceptions.

5 Summary

Over the course of 10 weeks, we studied how 24 participants used smartcards in multi-factor authentication. We had three main goals for the study. First, we wanted to learn how users would use the smartcards in their everyday work processes. All participants quickly became confident using the smartcards and reported them easier to use than password authentication. One consistent problem was that many participants forgot to use their smartcards to login, lock, or unlock their computers during the beginning of the study. One reason was because they had not yet developed a habit for using their smartcards; another reason was that the form factor of the smartcard reader also had an effect on participants forgetting their smartcards.

Second, we wanted to learn how users' work processes might change to accommodate smartcard use. We found two ways smartcards changed the way some of our participants worked. First, the physical presence of new hardware to interact with had an effect on user behavior with the smartcard system. Some participants felt the location of their smartcard readers was the cause of forgetting their smartcards in the readers. They experimented with the location and form factor of their smartcard readers until they were satisfied with their setup. We also describe one participant who developed a novel strategy to help her consistently remember her smartcard.

Second, digital signatures and encryption added an extra element to participants' document and email usage. Several participants experimented with digital signatures and encryption to see how they could incorporate the functionality into their work processes. However, few participants had a need for digital signatures and encryption.

Third, we were interested in the user benefits and drawbacks of using smartcards in authentication. The greatest perceived benefit of using smartcards was the use of a PIN in replacement of a password. Participants immediately noticed the difference between a shorter numeric PIN compared to the longer alpha-numeric-special character-password they were used to. Participants also appreciated that the same PIN was used for authenticating to multiple accounts, alleviating the need for complex password management practices. The greatest drawback to using smartcards was the lack of authentication support for more applications. The few participants who had trouble integrating the smartcard into their work processes used the smartcard only to authenticate to their computers. These participants experienced more overhead for smartcard use with fewer benefits than the participants who used the smartcards to authenticate to multiple systems.

Overall, participants had a positive experience with the smartcards and most indicated they would continue using the smartcards voluntarily and would even recommend using smartcards to their colleagues. It was interesting to see that participants' perceptions of the value of smartcards were related to personal benefits gained, such as an alternative to managing passwords, over the institutional benefit from increased security of a multi-factor authentication method.

Our multi-method approach provided us a richer understanding of smartcard use that could not be attained through traditional laboratory testing. While each method contributed to the understanding of our participants' behavior and perceptions, our experience provided lessons to further improve the methods for future or similar work.

Acknowledgements. We would like to thank Serge Egelman for his comments.

References

1. Arora, S.: National e-ID card schemes: A European overview. Information Security Technical Report, 13(2), 46-53 (2008).
2. Aussel, J.: Smartcards and Digital Security. Computer Network Security, 1, 42-56 (2007).
3. 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).
4. Brainard, J., Juels, A., Rivest, R.L., Szydlo, M., Yung, M.: Fourth-Factor Authentication: Somebody You Know. In proceedings of ACM CCS, 168-178 (2006).
5. 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).
6. Florencio, D. and Herley, C.: A large-scale study of web password habits. In proceedings of ACM Conference on the World Wide Web, 657-666 (2007).

7. Herley, C.: So Long and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In proceedings of New Security Perspectives Workshop 2009 (2009).
8. 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/
9. Information Technology Sector Coordinating Council.: Response to White House Cyber Review Questions. ITSCC March 20, 2009 (2009). http://www.it-scc.org/documents/itscc/ITSCCandCommunicationsSCCJointResponsetotheWhiteHouseCyberspacePolicyReview_3_20_2009.pdf
10. Inglesant, P.G. and Sasse, M.A.: The true cost of unusable password policies: password use in the wild. In proceedings of ACM Conference on Computer-Human Interaction, 383-392 (2010).
11. 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).
12. Jakobsson, M., Shi, E., Golle, P., and Chow, R.: Implicit Authentication for Mobile Devices. In proceedings of USENIX Workshop on HotSec (2009).
13. 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).
14. 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).
15. National Institute of Standards and Technology: Personal identity verification (PIV) for federal employees and contractors. FIPS PUB 201-1 (2006).
16. O'Gorman, L.: Comparing Passwords, Tokens, and Biometrics for User Authentication. Proc. IEEE 2003, 91(12), 2019-2040 (2003).
17. 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).
18. Sasse, M.A., Brostoff, S. and Weirich, D.: Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122-131 (2001).
19. Sasse, M.A.: Usability and Trust in Information Systems. Cyber Trust & Crime Prevention Project. University College London (2004).
20. Schechter, S. E., Dhamija, R., Ozment, A., and Fischer, I.: The Emperor's New Security Indicators. In proceedings of IEEE Symposium on Security & Privacy 2007, 51-65 (2007).
21. Schechter, S., Egelman, S., and Reeder, R.W. (2009). It's not what you know, but who you know: a social approach to last-resort authentication. Proc. ACM CHI 2009, 1983-1992.
22. 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).
23. Summers, W. C. and Bosworth, E.: Password policy: the good, the bad, and the ugly. In proceedings of WISICT 2004, 1-6 (2004).
24. 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).
25. 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>.
26. Weir, C.S., Douglas, G., Richardson, T., and Jack, M.: Usable security: User preferences for authentication methods in eBanking and the effects of experience. Interacting with Computers, 22(3), 153-164 (2010).