RC 23910 (W0603-080), 10 March 2006, Rev. 1, 26 May 2006
Computer Science

IBM Research Report

Privacy and Security Threat Analysis of the Federal Employee Personal Identity Verification (PIV) Program

Paul A. Karger
IBM Research Division
Thomas J. Watson Research Center
P. O. Box 704
Yorktown Heights, NY 10598, USA

Research Division
Almaden – Austin – Beijing – Delhi – Haifa – T.J. Watson – Tokyo – Zurich

This paper has been accepted for presentation at the 2006 Symposium on Usable Privacy and Security (SOUPS), July 12-14, 2006, Carnegie-Mellon University, Pittsburgh, PA.

Privacy and Security Threat Analysis of the Federal Employee Personal Identity Verification (PIV) Program

Paul A. Karger
IBM Research Division, Thomas J. Watson Research Center
PO Box 704, Yorktown Heights, NY 10598, USA
karger@watson.ibm.com

ABSTRACT

This paper is a security and privacy threat analysis of new Federal Information Processing Standard for Personal Identity Verification (FIPS PUB 201). It identifies some problems with the standard, and it proposes solutions to those problems, using standardized cryptographic techniques that are based on the Internet Key Exchange (IKE) protocol [16]. When the standard is viewed in the abstract, it seems to effectively provide security and privacy, because it uses strong cryptographic algorithms. However, when you examine the standard in the context of potential user scenarios regarding its use; security, privacy, and usability problems can be identified. User scenarios are employed to provide the context for the identification of these problems, and the technical solutions are described to address the issues raised.

Categories and Subject Descriptors

C.3 [**Computer Systems Organization**]: Special-Purpose and Application-Based Systems—*smart cards*; K.6.5 [**Computing Milieux**]: Management of Computing and Information Systems—*Security and Protection, authentication*

General Terms

security

Keywords

personal identification, privacy, smart cards

1. INTRODUCTION

In August 2004, President Bush issued Homeland Security Presidential Directive 12 (HSPD 12) [5] calling for a government-wide standard for "secure and reliable forms of identification" for both federal employees and contractors. By "secure and reliable", the directive means identification that "(a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process."

In response to this HSPD, the National Institute of Standards and Technology (NIST) developed Federal Information Processing Standard Publication (FIPS PUB) 201 [33] on Personal Identity Verification (PIV), as well as a series of accompanying publications including [12, 3] to assist in the implementation. HSPD 12 imposed very short schedules for the development of FIPS PUB 201 and for the initial deployment of identification cards that met the standard.

This paper is a security and privacy threat analysis of FIPS PUB 201. It identifies some problems with the standard, and it proposes solutions to those problems, using standardized cryptographic techniques that are based on the Internet Key Exchange (IKE) protocol [16].

The organization of the paper is as follows: First, the paper presents an overview of FIPS PUB 201. Then it discusses the increased vulnerability of contactless smart cards, when compared to contact smart cards. Next, several potential vulnerabilities in FIPS PUB 201 of varying severities are shown. FIPS PUB 201 cards are then contrasted with electronic passports. The paper then presents a new cryptographic protocol that can solve the privacy and security problems of both FIPS PUB 201 and electronic passports. The paper concludes with a discussion of why these kinds of vulnerabilities can easily occur and makes recommendations on how NIST could proceed.

2. OVERVIEW OF FIPS PUB 201

FIPS PUB 201 actually defines two kinds of Personal Identity Verification (PIV) cards: PIV-I and PIV-II. PIV-I cards meet the control and security requirements of HSPD 12, while PIV-II cards meet the additional requirements for interoperability between federal agencies. The purpose of the distinction between PIV-I and PIV-II cards is to permit quicker agency compliance with HSPD 12. This paper will focus only on the PIV-II cards which are to be implemented using smart card chips. For the remainder of this paper, we assume that the term "PIV card" refers to a PIV-II card.

Printed on each PIV card will be the name and a photograph of the card holder, the cardholder's organization, a serial number, an expiration date, and a variety of other agency-specific information. The card will contain both contact smart card and contactless smart card interfaces, implemented either with a single dual-interface smart card chip or with two smart card chips. Both contact and contactless interfaces are provided, because each provides advantages that can be exploited by federal agencies in their deployment of PIV cards. Contact interfaces provide higher levels of security, because they avoid the use of radio communications. However, contact interfaces are less convenient to use, and the electrical contacts on the card can wear out with frequent use. Contactless

Symposium On Usable Privacy and Security (SOUPS) 2006, July 12-14, 2006, Pittsburgh, PA, USA.

interfaces are much easier and quicker to use, as the card holder needs only to wave the card near the reader to have the information read. However, contactless interfaces have additional security risks, discussed below in section 3.

At a minimum, each smart card chip shall store a personal identification number (PIN) known by the card holder, a Card Holder Unique Identifier (CHUID), PIV authentication data consisting of an asymmetric key pair and corresponding certificate, and two biometric fingerprints. Each agency can store additional optional information in the smart card chip, including cryptographic keys for digital signatures, key management, additional physical access control applications, card management, etc.

3. CONTACTLESS IMPLICATIONS

This section will examine a few user scenarios to highlight the security and privacy differences between contactless and contact smart cards.

FIPS PUB 201 [33] specifies that the PIV card shall have both contact and contactless smart card interfaces. The contactless interfaces are specified by ISO 14443-4 [18]. Contactless smart cards communicate over radio communications and are powered by transmissions from the reader itself. In many ways, contactless smart cards are similar to radio frequency identification (RFID) tokens, although there are detailed technical differences explained in [36]. Because of the use of radio, contactless smart cards, like RFID tokens, face more serious security and privacy threats than do contact smart cards that must be inserted into a reader before they can be accessed.

In a typical user scenario for a contact interface, the card holder will approach a contact smart card reader and insert his or her card into a slot in the reader. For PIV cards, this reader is likely to be at entrance to a federal agency. A PIV card holder is quite unlikely to insert his or her card into a unauthorized reader. There have been attacks in which criminals created bogus Automatic Teller Machines (ATMs) into which unsuspecting customers inserted their cards, but who would insert a PIV card into an ATM? If PIV cards became multi-application in the future, however, this threat of bogus readers could become more real.

By contrast, the user scenario for an attack on a contactless interface can occur anywhere. The card holder could be at home or walking down the street or actually using the contactless card at a legitimate contactless reader at work. A contactless smart card could be powered and accessed while the card is stored in the pocket of the card holder. While reliable access to contactless smart cards is only guaranteed over a small number of centimeters, an attacker will be satisfied with a much lower level of reliability and can therefore achieve access at considerably greater distances.

This problem of eavesdropping at a distance has been most studied in the context of a passport scenario. Yoshida [43] and the Smart Card Alliance [37] both report successful eavesdropping on contactless smart cards at a distance of 9 meters. Kfir and Wool [26] report successful attacks at 50 meters. It is believed that eavesdropping is easier when the card is actually in use communicating with a legitimate reader, as in when a passport holder presents the contactless passport to an immigration officer at the airport. In this case, the attacker is not required to provide power to the contactless smart card, only to listen to the signals. However, if the attacker is willing to transmit at illegally high power levels, then attacks on cards that are not in use are possible at a distance. Since the attack consists only of some radio waves, the card holder is extremely unlikely to realize that eavesdropping has occurred.

As a result of the possibility of this kind of eavesdropping, it is of major importance that contactless smart card communications be fully encrypted. However, FIPS PUB 201 only requires that the PIV card store one asymmetric key pair, and specifies in section 4.3 that "cryptographic operations with this key are performed only through the contact interface." While FIPS PUB 201 permits an agency to store additional keys on the card and to encrypt the contactless communications with such keys, the use of encryption on the contactless interface is not required. FIPS PUB 201 contains no rationale for not requiring encryption, and since the contactless interface is more in need of encryption than the contact interface, the lack of requirements in this section are quite curious.

4. CARD HOLDER UNIQUE IDENTIFIER (CHUID)

The Card Holder Unique Identifier is specified in [39] and further refined in [12]. The CHUID includes the Federal Agency Smart Credential Number (FASC-N) which is based on a much older specification from the DoD Security Enterprise Integration Working Group (SEIWG-12) [35]. The original SEIWG-12 specification used the card holders social security account number (SSAN) which could have contributed to identify theft. The use of the SSAN is strongly discouraged in [39, section 6.1] specifically to avoid this threat of identity theft.

In addition to the FASC-N, the CHUID contains a number of other fields of information about the card holder, the most relevant of which is the agency code that indicates for which federal agency does the card holder work.[1]

Section 4.1.6 of FIPS PUB 201 [33] states that "a read of a PIV CHUID is not considered a privileged operation." The result of this assumption was a design decision that it was safe to transmit the CHUID in unencrypted form from the PIV card to the reader, prior to authentication. As we shall see in the next subsections, this assumption is invalid. The CHUID does contain sensitive information that can lead to serious problems over the contactless interface.

4.1 CHUID Problems in Nov. 2004 Version

In the draft of FIPS PUB 201 that was released for public comment [32] in November 2004, the CHUID also included a field called "Position Sensitivity". In table 5-2 of the November 2004 draft, Position Sensitivity was correlated with the level of background investigation carried out on the card holder. This raised a serious potential problem, as the level of background investigation is directly correlated with the level of security clearance that the employee held. This means that an eavesdropper could determine the level of security clearance held by a federal employee from a distance. That could put highly cleared federal employees at serious risk, particularly in overseas assignments.

Karger [23] and Bailey [2] pointed out these problems to NIST in January 2005[2] and recommended that the CHUID only be transmitted in encrypted form.[3]

[1]Government contractors get different codes to specify employers (as opposed to Federal agencies), and these codes are not guaranteed to be unique.

[2]Karger and Bailey's presentations were independently prepared and accepted for a public meeting held in January 2005 on Privacy and Policy issues in FIPS PUB 201. However, concerns over the sensitive nature of the vulnerabilities disclosed led to Karger's work being presented only in private meetings with the government.

[3]Bailey also suggested the use of a Faraday cage to protect the card when not in use or the use of a button on the card to enable the contactless interface only when the card holder specified. These are good suggestions and should be considered. However, these protections would not protect against eavesdropping the CHUID when the card was in use at a legitimate contactless reader.

4.2 CHUID Problems in Feb. 2005 Version

As a result of the comments from Karger and Bailey, NIST modified the CHUID to eliminate the position sensitivity field. NIST also added a special-risk security provision on page v of FIPS PUB 201. This provision allows the head of a department or independent agency to identify a limited number of individuals whose overseas assignments expose them to particular severe threats. Such individuals could be issued special credentials without wireless or biometric capabilities. However, the number of such credentials must be minimized, and they are only permitted outside the Continental US (CONUS).

While the changes that NIST made to respond to Karger and Bailey are good, as far as they go, they do *not* stop all the serious threats to the card holders.

The CHUID also includes the agency code in the FASC-N and the optional organization code in the CHUID.[4] These agency codes are fully specified and publicly available in [3], and they provide a very detailed breakdown of specific organizations. Agencies are not large scale organizations like the Department of Commerce or the Air Force. Rather the agency/organization codes are very fine grained and can identify organizations like the Animal and Plant Health Inspection Service (code 12K3) or the Air Force Command and Control (C2) & Intelligence, Surveillance and Reconnaissance (code 571A). Clearly an eavesdropper might be much more interested in an employee of the latter agency than of the former. Even without the position sensitivity field, an attacker can assume that an employee of agency 571A will likely have a much higher security clearance than an employee of agency 12K3. Such information would be of value to an attacker either overseas or within CONUS.

The solution to the problem was not to eliminate the position sensitivity field or to establish a special risk security provision for a selected set of employees who serve overseas. The proper solution is to protect the contents of the CHUID from eavesdropping using encryption as shown in section 8.

Note that protecting the CHUID contents will not eliminate all possible threats. Consider the user scenario in which a terrorist wishes to exploit the ID card. For example, in the 1985 hijacking of TWA Flight 847 [7], the terrorists found the ID card of US Navy diver Robert Stethem and brutally murdered him. No amount of encryption will protect against an attack of that kind in which the terrorist can see what is printed on the ID card.

However, if you consider a user scenario in which the terrorist does not have physical possession of the ID card, then CHUID protection can be effective. Terrorists like the Washington DC snipers [17] might wish to attack federal employees or employees of a particular agency. In that scenario, eavesdropping on the CHUID might be very useful to help the snipers select a target. Similarly, if an espionage recruiter is attempting to find a likely target, again eavesdropping on the CHUID in a Washington, DC restaurant or bar might prove very effective.

5. PIN PROBLEMS

The CHUID is not the only data item normally transmitted in unencrypted form. The authentication data that is to be compared against the user's PIN is also always transmitted in the clear, as specified in the VERIFY APDU in section 2.3.3.2.1 of [12]. This problem is mitigated by a requirement in section 7 that says, "Cryptographic protocols using asymmetric keys that require PIN shall not be used on the contactless interface." However, this requirement does NOT state that the PIN shall not be used on the contactless interface without the use of asymmetric keys. That option is left to the agencies, and could easily lead to the exposure of the PIN in unencrypted form over the contactless interface. FIPS PUB 201 needs a clear and unequivocal requirement that the PIN (or a value to be compared with the PIN) never be transmitted across the contactless interface in unencrypted form.

[4]The distinctions between the agency code and the organization code are due to the FASC-N being specified in BCD for backwards compatibility reasons. NIST hopes to eventually phase these out and replace them with a global unique ID, based on an IPV6 address for the agency. Use of a global unique ID would not change any of the security or privacy issues in this paper.

6. FAKE FINGERS

FIPS PUB 201 [33] provides for unattended biometric authentication in section 6.2.3.1 with further detailed user scenarios in [12, Appendix C]. An unattended biometric reader might be used to control access to a building, while saving the costs of having a security guard present at all times.

However, these scenarios do not consider the possibility of an attacker who has stolen a PIV card and obtained the PIN, perhaps because the legitimate card holder wrote it down. The unstated assumption is that in such a case, the biometric fingerprint check would defeat the attacker. However, several papers [31, 30, 40] have demonstrated the effectiveness of fake "gummy" fingers against most commercial fingerprint readers, even those with "liveness" checks. In an attended biometric check, the guard can be trained to watch for fake fingers and ensure that a real finger is used. However, in an unattended scenario, the use of fake fingers becomes easy. Worse still, as biometric fingerprint checks become more common, a weakness in one biometric credential could affect the security of other credentials. Kc and Karger [25, section 3.2.2] discuss how stealing a digitized fingerprint off a passport could be significantly easier than lifting a fingerprint off of something like a drinking glass, because there would no difficulties with smearing. Kc and Karger show how a fake fingerprint could be used to attack the unattended Malaysian boarder crossing system [22].

7. COMPARISON WITH ICAO MRTDS

It is interesting to compare the security and privacy of PIV cards with the comparable features for the new electronic passports that are beginning to be deployed in compliance with specifications [27, 10] set by the International Civil Aviation Organization (ICAO) for Machine Readable Travel Documents (MRTDs). The security and privacy features of ICAO MRTDs have come under some legitimate criticism [21, 26, 25, 43].

Both ICAO MRTDs and PIV cards use a contactless interface, but the ICAO MRTDs only use contactless - they have no contact interface. In general, the cryptographic protocols used on PIV cards are stronger than the ICAO protocols. The ICAO Basic Access Control keys have been shown to have insufficient entropy by Witteman [42] who was able to brute force the cryptographic keys of a Dutch passport in about two hours on a standard PC. By contrast, the strength of cryptographic keys required [34] for use in PIV cards is quite adequate, and NIST recommends increasing the minimum key sizes over time.

Both ICAO MRTDs and PIV cards suffer from some information not being encrypted over the contactless interface. In the case of ICAO MRTDs, the use of encryption at all is completely optional, and an electronic passport that transmits all of its data, including biometrics to any eavesdropper is compliant with the standards. Fortunately, many countries, including the US, have committed [44] to the use of encryption to prevent this kind of casual eavesdropping. PIV cards do a much better job of protect-

ing the biometrics by always requiring the use of strong cryptography when transmitting biometric information. However, FIPS PUB 201 [33] requires that the CHUID be transmitted in the clear, and this leads to the problems discussed above in section 4.

Thus, the ICAO MRTDs and the PIV cards both suffer from cryptographic problems and need some significant improvements, but on balance, the PIV cards have fewer vulnerabilities.

Consider a user scenario of a terrorist wishing to gain access to a facility protected only with an unattended biometric reader. The terrorist kidnaps an employee who works in the building. The employee is carrying both a PIV card and an electronic passport. The terrorist extracts the digitized fingerprint biometric from the passport, and uses it to make a fake finger. Since the fingerprint is already digitized, it is likely to produce a higher quality fake finger than using the real finger. After all, the digitized version is already known to work in fingerprint readers. Under torture, the employee is forced to reveal the PIN. The terrorist now has possession of the PIV card, knows the PIN, and can use the fake finger to pass the biometric checks to gain access to the facility.

8. SOLVING THE CHUID EXPOSURE

The right way to solve the CHUID exposure is to fully encrypt all traffic between the PIV card and its readers, regardless of whether such traffic goes over the contact or the contactless interface. However, fully encrypted traffic could lead to privacy exposures for the card holder, depending on how the cryptographic keys are negotiated between the card and the reader.

The German DIN standards [8, 9] for digital signature cards[5] attempt to protect such traffic between smart cards and reader, but they have the disadvantage that the card must reveal its identity and certificate in the clear before it has verified the credentials of the reader. This could be viewed as a violation of the privacy of the card holder - the identity and certificate of the card are revealed, not just to the reader, but also to anyone eavesdropping on the communications between the reader and the card.

To avoid these privacy problems, IBM developed the Caernarvon authentication protocol [38] that preserves the card holder's privacy by revealing nothing until the reader has been authenticated. Very briefly, the Caernarvon protocol generates a Diffie-Hellman[6] session key first to protect all subsequent communications from external eavesdroppers. Then it requires the reader to authenticate itself to the chip, and only after the chip has determined that the reader is authorized, does the chip reveal any information at all about the card holder.

The Caernarvon authentication protocol [38] was specifically designed to protect the privacy of a smart card holder and is based on the SIGMA family [28] of protocols that form the basis of the Internet Key Exchange Protocol (IKE) [16]. Not only are the SIGMA protocols a widely used standard, they have also been formally proven correct [6]. IBM has chosen not to assert any IP claims on the protocol, to ensure that it can be freely used in standards. As a result, the Caernarvon protocol is being adopted [1] for use by CEN, the European Committee for Standardization and will likely go on to ISO standardization after the CEN process has completed. A summary of the Caernarvon authentication protocol can be found in the Appendix, although for a full analysis of the protocol, the reader is directed to the published paper [38].

IBM has also recommended the Caernarvon authentication protocol as a solution [25] to the privacy and security problems in the ICAO MRTD specifications.

[5]The German digital signature card standards are based on ISO 11770-3 [20, section 6.7, Key Agreement Mechanism 7].

[6]Diffie-Hellman was the first public-key algorithm openly published in 1976 [11]. The Diffie-Hellman algorithm was first developed by M. J. Williamson at the Communications-Electronics Security Group (CESG) in the UK and published internally somewhat later in [41], but that work remained classified until much later [14]. It gets its security from the difficulty of calculating discrete logarithms in a finite field, as compared with the ease of performing exponentiation calculations in the same field.

9. CONCLUSIONS

We have seen that under some user scenarios, particularly those using contactless interfaces, that the FIPS PUB 201 PIV cards have privacy and security vulnerabilities. While many of these problems could be avoided by eliminating the contactless interfaces, that would also severely limit how the different federal agencies could use the PIV cards. These issues are serious, because they impinge on the requirements specified in HSPD 12 [5] that the PIV cards be "strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation."

We have shown how the Caernarvon authentication protocol [38] can solve most of the vulnerabilities, without giving up flexibility is the use of PIV cards.

9.1 Wireless Protocols are Hard to Secure

It is not the intent of this paper to be overly harsh on the process followed by NIST to develop the standards. Getting wireless security protocols to be secure is a very hard task, and NIST was given a very short time in which to complete FIPS PUB 201. From the track record of other major wireless security protocol developments, it is not surprising that some problems remain. Among the protocols that have had similar problems are 802.11 [13], Cellular Digital Packet Data (CDPD) [15], cell phones [29], Intelligent Transport Systems (ITS) [24], and many others. These problems arise, because the designers of a wireless protocol frequently focus on the issues of getting the protocol to work and may not have to address many of the subtle security and privacy implications. Such projects need to do comprehensive vulnerability analyses to ensure not only the security of the protocols themselves, but also that side effects of the protocols do not create problems for other systems. The problem here was not the choice of cryptographic algorithms or protocols, but rather that certain critical information was left unencrypted.

9.2 Usability

Analysis of a security or privacy system for usability normally focuses on the end users. FIPS PUB 201 ID cards are very easy to use. You just waive them near the contactless reader. This is excellent usability for the card holder. However, there are serious issues for the federal agencies who wish to deploy these cards.

FIPS PUB 201 specifies only a minimal set of mandatory cryptographic functions, and in the process, leaves some critical information exposed and unencrypted. However, it also provides a wide variety of cryptographic options so that the federal agencies can devise their own cryptographic extensions. We have also seen that designing secure wireless cryptographic protocols is hard. Without careful examination of many different user scenarios, it is very easy to leave subtle but potentially fatal vulnerabilities.

This paper has proposed the mandatory use the Caernarvon authentication protocol as a way to use a formally proven protocol to address many if not all of the possible user scenarios. Perhaps the real problem is that FIPS PUB 201 provides too much cryptographic flexibility. Choosing a single authentication protocol that has been proven correct makes it easier to ensure that not just the usage scenarios specified in FIPS PUB 201 are secure, but also that

agency-specific usage scenarios that are not yet specified will also be secure, without requiring such a high cryptographic skill level on the part of agency developers.

It would be useful and interesting to conduct further research to see if, by reducing the cryptographic options to just the Caernarvon authentication protocol, that there are any remaining agency-specific usage scenarios that the Caernarvon authentication protocol cannot handle.

10. ACKNOWLEDGMENTS

I must acknowledge the many people who commented on this and earlier versions of this work, including David Toll, Sam Weber, Charles Palmer, Elaine Palmer, Stu Feldman, Tom Hissam, Suzanne McIntosh, John McKeon, Michael Karasick, and the anonymous reviewers of the paper.

11. REFERENCES

[1] Application interface for smart cards used as secure signature creation devices - part 1: Basic requirements. CWA 14890-1, Comité Européen de Normalisation (CEN), Brussels, Belgium, March 2004. URL: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14890-01-2004-Mar.pdf.

[2] Dan Bailey. Contactless threats to FIPS 201 systems. In *Public Meeting Addressing Privacy and Policy Issues in a Common Identification Standard for Federal Employees and Contractors*, Washington, DC, 19 January 2005. National Institute of Standards (NIST). URL: http://csrc.ncsl.nist.gov/piv-program/workshop-Jan19-2005/Bailey.pdf.

[3] William C. Barker and Hildegard Ferraiolo. Codes for the identification of federal and federally assisted organizations. NIST Special Publication 800-87, Version 1.0, National Institute of Standards and Technology, Gaithersburg, MD, January 2006. URL: http://csrc.ncsl.nist.gov/publications/nistpubs/800-87/sp800-87-Final.pdf.

[4] David E. Bell and Leonard J. LaPadula. Computer security model: Unified exposition and multics interpretation. Technical Report ESD–TR–75–306, The MITRE Corporation, Bedford, MA, USA, HQ Electronic Systems Division, Hanscom AFB, MA, USA, June 1975.

[5] George W. Bush. Policy for a common identification standard for federal employees and contractors. Homeland Security Presidential Directive Hspd-12, The White House, Washington, DC, 27 August 2004. URL: http://csrc.nist.gov/policies/Presidential-Directive-Hspd-12.html.

[6] Ran Canetti and Hugo Krawczyk. Security analysis of IKE's signature-based key-exchange protocol. In *Advances in Cryptology - Crypto 2002*, volume 2045 of *Lecture Notes in Computer Science*, pages 143–161, Santa Barbara, CA, 2002. Springer-Verlag.

[7] Kurt Carlson. *One American Must Die: A Hostage's Personal Account of the Hijacking of Flight 847*. Congdon & Weed, 1986.

[8] Chipcards with digital signature application/function according to SigG and SigV - part 1: Application interface. DIN V66291-1, Secretariat: DIN Deutsches Institut für Normung e.V, Berlin, 15 December 1998.

[9] Chipcards with digital signature application/function according to SigG and SigV - part 4: Basic security services. DIN V66291-4, Secretariat: DIN Deutsches Institut für Normung e.V, Berlin, 17 October 2000.

[10] Development of a logical data structure (LDS) for optional capacity expansion technologies. LDS 1.7–2004–05-18, Revision 1.7, International Civil Aviation Organization, Montreal, Quebec, Canada, 18 May 2004. URL: http://www.icao.int/mrtd/download/technical.cfm.

[11] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[12] James F. Dray, Scott B. Guthery, and Teresa Schwarzhoff. Interfaces for personal identity verification. NIST Special Publication 800-73, National Institute of Standards and Technology, Gaithersburg, MD, April 2005. URL: http://csrc.ncsl.nist.gov/publications/nistpubs/800-73/SP800-73-Final.pdf.

[13] Jon Edney and William A. Arbaugh. *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*. Addison-Wesley, Boston, MA, 2004.

[14] J. H. Ellis. The story of non-secret encryption. Technical report, Communications-Electronics Security Group (CESG), Cheltenham, UK, 1987. URL: http://www.cesg.gov.uk/publications/media/nsecret/ellis.pdf.

[15] Yair Frankel, Amir Herzberg, Paul A. Karger, Hugo Krawczyk, Charles A. Kunzinger, and Moti Yung. Security issues in a CDPD wireless network. *IEEE Personal Communications*, 2(4):16–27, August 1995.

[16] D. Harkins and D. Carrel. The internet key exchange (IKE). RFC 2409, November 1998. URL: ftp://ftp.rfc-editor.org/in-notes/rfc2409.txt.

[17] Sari Horwitz and Michael Ruana. *Sniper: Inside the Hunt for the Killers Who Terrorized the Nation*. Random House, New York, 2003.

[18] Identification cards - contactless integrated circuit(s) cards - proximity cards - part 4: Transmission protocol. ISO/IEC 14443-4, International Standards Organization, Geneva, Switzerland, 2000.

[19] Information technology - identification cards - integrated circuit(s) cards with contacts - part 4: Inter-industry commands for interchange. ISO/IEC 7816-4, International Standards Organization, Genève, 1995.

[20] Information technology - security techniques - key management - part 3: Mechanisms using asymetric techniques. ISO/IEC 11770-3, International Organization for Standardization, Genève, 1 November 1999.

[21] Ari Juels, David Molnar, and David Wagner. Security and privacy issues in e-passports. In *SecureComm 2005, First International Conference on Security and Privacy for Emerging Areas in Communication Networks*, Athens, Greece, 5–9 September 2005. URL: http://www.cs.berkeley.edu/~daw/papers/epassports-sc05.pdf.

[22] Dato' Mohd Jamal Kamdi. The Malaysian electronic passport. In *Twelfth Meeting of the Facilitation Division*, Cairo, Egypt, 22 March - 2 April 2004. International Civil Aviation Organization (ICAO). URL: http://www.icao.int/icao/en/atb/fal/fal12/presentations.htm.

[23] Paul A. Karger. FIPS PUB 201 security and privacy recommendations. Report RC23871 (W0501-049), IBM Corporation, Thomas J. Watson Research Center, Yorktown Heights, NY, 14 January 2005. URL: http://domino.watson.ibm.com/library/CyberDig.nsf/Home.

[24] Paul A. Karger and Yair Frankel. Security and privacy threats

to ITS. In *Proceedings of the Second World Congress on Intelligent Transport Systems '95 Yokohama*, volume V, pages 2452–2458, Yokohama, Japan, 9–11 November 1995. VERTIS: Vehicle, Road and Traffic Intelligence Society.

[25] Gaurav S. Kc and Paul A. Karger. Preventing attacks on machine readable travel documents (MRTDs). Report 2005/404, Cryptology ePrint Archive, 11 April 2006. URL: http://eprint.iacr.org/2005/404.pdf.

[26] Ziv Kfir and Avishai Wool. Security and privacy issues in e-passports. In *First International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm 2005)*, pages 47–58, Athens, Greece, 5–9 September 2005. URL: http://eprint.iacr.org/2005/052.

[27] Tom A. F. Kinneging. PKI for machine readable travel documents offering ICC read-only access. Version 1.1, International Civil Aviation Organization, Montreal, Quebec, Canada, 1 October 2004. URL: http://www.icao.int/mrtd/download/technical.cfm.

[28] Hugo Krawczyk. SIGMA: the 'SIGn-and-MAc' approach to authenticated diffie-hellman and its use in the IKE protocols. In *Advances in Cryptology – CRYPTO 2003 Proceesings*, volume 2729 of *Lecture Notes in Computer Science*, pages 399–424, Santa Barbara, CA, 17-21 August 2003. Springer–Verlag.

[29] Susan Kumpf and Nora Russell. Getting the jump on fraud. *Cellular Business*, 9(10):24–26, October 1992.

[30] Tsutomu Matsumoto. Gummy and conductive silicone rubber fingers: Importance of vulnerability analysis. In *Advances in Cryptology: ASIACRYPT 2002*, pages 574–575, Queenstown, New Zealand, 1–5 December 2002. Lecture Notes in Computer Science, Vol. 2501, Springer Verlag.

[31] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. Impact of artificial "gummy" fingers on fingerprint systems. *Proceedings of the SPIE, Optical Security and Counterfeit Deterrence Techniques IV*, 4677:275–289, 24–25 January 2002. URL: http://cryptome.org/gummy.htm.

[32] Personal identity verification (PIV) for federal employees and contractors: Public draft. FIPS PUB 201, National Institute of Standards and Technology (NIST), Gaithersburg, MD, 8 November 2004. URL: http://csrc.nist.gov/publications/drafts/draft-FIPS_201-110804-public1.pdf.

[33] Personal identity verification (PIV) for federal employees and contractors. FIPS PUB 201, National Institute of Standards and Technology (NIST), Gaithersburg, MD, 25 February 2005. URL: http://csrc.ncsl.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf.

[34] W. Timothy Polk, Donna F. Dodson, and William E. Burr. Cryptographic algorithms and key sizes for personal identity verification. NIST Special Publication 800-78, National Institute of Standards and Technology, Gaithersburg, MD, April 2005. URL: http://csrc.ncsl.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf.

[35] Prime item product function specification for magnetic stripe credentials (MSC). SEIWG 012, U.S. Department of Defense, Security Enterprise Integration Working Group (SEIWG), Washington, DC, 28 February 1994.

[36] RFID tags and contactless smart card technology: Comparing and contrasting applications and capabilities. Technical report, Smart Card Alliance, Princeton Junction, NJ, 17 December 2004. URL: http://www.smartcardalliance.org/pdf/alliance_activities/rfidvscontactless_final_121704.pdf.

[37] RFID tags, contactless smart card technology and electronic passports: Frequently asked questions. Technical report, Smart Card Alliance, Princeton Junction, NJ, 3 January 2005. URL: http://www.smartcardalliance.org/pdf/alliance_activities/RFID_Contactless_Smart_Cards_FAQ_FINAL_010305.pdf.

[38] Helmut Scherzer, Ran Canetti, Paul A. Karger, Hugo Krawczyk, Tal Rabin, and David C. Toll. Authenticating mandatory access controls and preserving privacy for a high-assurance smart card. In *8th European Symposium on Research in Computer Security (ESORICS 2003)*, pages 181–200, Gjøvik, Norway, 13–15 October 2003. Lecture Notes in Computer Science, Vol. 2808, Springer Verlag.

[39] Technical implementation guidance: Smart card enabled physical access control systems. Version 2.2, Physical Access Interagency Interoperability Working Group, Government Smart Card Interagency Advisory Board, Washington, DC, 30 July 2004. URL: http://www.smart.gov/information/TIG_SCEPACS_v2.2.pdf.

[40] Lisa Thalheim, Jan Krissler, and Peter-Michael Ziegler. Body check: Biometric access protection devices and their programs put to the test. *c't - magazin für computertechnik*, page 114, November 2002. URL: http://www.heise.de/ct/english/02/11/114/.

[41] M. J. Williamson. Thoughts on cheaper non-secret encryption. Technical report, Communications-Electronics Security Group (CESG), Cheltenham, UK, 10 August 1976. URL: http://www.cesg.gov.uk/publications/media/nsecret/cheapnse.pdf.

[42] Marc Witteman. Attacks on digital passports. In *What the Hack*, Liempde, near Den Bosch, The Netherlands. URL: http://wiki.whatthehack.org/index.php/Track:Attacks_on_Digital_Passports.

[43] Junko Yoshida. Tests reveal e-passport security flaw. *Electronic Engineering Times*, (1336):1, 30 August 2004. URL: http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=45400010.

[44] Kim Zetter. Feds rethinking RFID passport. *Wired News*, 26 April 2005. URL: http://www.wired.com/news/privacy/0,1848,67333,00.html.

APPENDIX

A. CAERNARVON AUTHENTICATION PROTOCOL

This appendix provides a brief summary of the Caernarvon authentication protocol. A much more complete analysis can be found in [38].

In addition to the privacy problems discussed in section 8, the protocols based on ISO 11770-3 also have the disadvantage that the number of bits transmitted in all the stages is somewhat larger than necessary. Minimizing the total number of bits transmitted is important, because some smart card readers will only communicate at 9600bps, and even ignoring the cost of computing the cryptographic operations, the time needed to transmit all the bits could become a serious problem in response time to the card holder.

To resolve both the privacy problems and to reduce the number of bits to be transmitted, the Caernarvon authentication protocol is based on the SIGMA design [28] and the Internet Key Exchange (IKE) standard [16]. This protocol offers several significant advantages:

1. The session key parameters are exchanged very early in the protocol, even before the authentication has been completed. In this way, the information exchanged in the protocol, including the peers' identities can be protected from third-party eavesdropping.
2. A discloses its identity and credentials to B first; B reveals its identity and credentials only after verifying those of A. This prevents revealing the card holder's identity to a reader that cannot be authenticated or that cannot prove that it is authorized for a particular mandatory access classes. Therefore, the card's identity is protected not only against eavesdropping, but also against an active (man-in-the-middle) attacker. The reader's identity is not protected against an active attacker, but presumably the reader has fewer privacy concerns than the card holder. Note that in all authentication protocols, one party must reveal its identity first, and that party's privacy will always be subject to active attacks of this kind.
3. IKE transmits fewer bits in total. This will improve performance on slow readers.
4. The SIGMA and IKE protocols followed here have been rigorously analyzed and proven correct [6], which is a major benefit in any system planning to be evaluated at the highest levels of the Common Criteria. In particular, see [28] for more details on the cryptographic rationale of these protocols and the subtle cryptographic attacks they prevent.

This section contains a cryptographic description of the authentication protocol used by Caernarvon. Note that in contrast to the protocol described in ISO 11770-3, the Caernarvon protocol starts as in unauthenticated Diffie-Hellman, and then authenticates the reader,A, before the card, B, exposes its identity. The crucial technical difference between these protocols is that in the case of the Caernarvon protocol, A can authenticate itself to B without having to know B's identity, while in the ISO protocol, A authenticates to B by signing B's identity (thus requiring the knowledge of B's identity by A before A can authenticate to B). A (the reader) and B (the Caernarvon card) share the Diffie-Helman public quantities p, q, and g.

Stage 1. A chooses a random number a with $1 \leq a \leq q-1$, computes a key token $K_A = g^a \bmod p$, and transmits it to B, as shown in Figure 1.

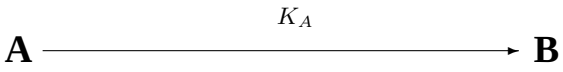

Figure 1: Authentication Stage 1: A sends a key token to B

Stage 2. B chooses a random number b with $1 \leq b \leq q-1$, computes a key token $K_B = g^b \bmod p$, and transmits it to A, as shown in Figure 2.

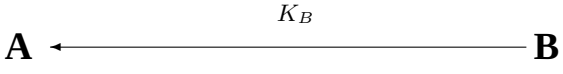

Figure 2: Authentication Stage 2: B sends a key token to A

At this point, neither A nor B has revealed his identity. However, they now can compute a mutual key K_{AB}. Using the mutual key K_{AB}, they can derive additional keys K_{ENC}, for encrypting messages and K_{MAC}, for computing message authentication codes (MACs).

Stage 3. A now sends its certificate to B by encrypting it with K_{ENC}. A now computes E_{01} as shown below:

$$E_{01} = 3DES_{K_{ENC}}(Cert(A))$$

A now transmits E_{01} together with its MAC to B, as shown in Figure 3.

Figure 3: Authentication Stage 3: A sends certificate to B

Stage 4. B responds with a challenge, as shown in Figure 4. From a strictly cryptographic perspective, stage 4 could be combined with stage 2, reducing the total number of message flows. However, this is a protocol for smart cards, and it must fit into the existing standard for smart card commands [19] and use the GET CHALLENGE and EXTERNAL AUTHENTICATE commands.

Figure 4: Authentication Stage 4: B sends challenge to A

Stage 5. A now computes E_1 as shown below:

$$E_1 = 3DES_{K_{ENC}}(A \| Sig_{SK_A}[K_A \| A \| RND.B \| K_B \| DH(g \| p \| q)])$$

A now transmits E_1 and a MAC of E_1 to B, as shown in Figure 5. The signature is a signature with message recovery, so all parameters in the signature can considered to be recoverable. The Diffie-Hellman key parameters are part of the signature in order to provide authenticity of the parameters. See [38] for details.

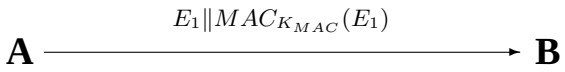

Figure 5: Authentication Stage 5: Authenticate A

At the conclusion of stage 5, B has authenticated A. It is at this point that the Caernarvon authentication protocol permits the card to make a security policy decision about whether it wishes to communicate with A or not. The security policy checks are done here, so that B can verify A's access rights, before revealing any privacy-sensitive information to A. While any security policy can be used here, the Caernarvon authentication protocol was specifically designed to support mandatory access controls for both commercial citekarger-wisac2000 and defense purposes [4].

Stage 6: B now verifies the MAC, decrypts E_1, and verifies the signature using A's public key PK_A. B has now authenticated A and knows that K_A and K_B are fresh and authentic. However at this point, while B knows there is no man-in-the-middle because B checked the signature from A, A does not know who he is talking

to, and hence is unsure if there may be a man-in-the-middle attack. B computes E_{02} (its encrypted certificate) and sends it to A, as shown in Figure 6.

$$E_{02} = 3DES_{K_{ENC}}(Cert(B))$$

Figure 6: Authentication Stage 6: B sends certificate to A

Stage 7. A sends a challenge to B, as shown in Figure 7. Just as for stage 4, strict cryptographic requirements could reduce the total number of message flows. However, once again, it is desirable to use the ISO standard [19] GET CHALLENGE and EXTERNAL AUTHENTICATE commands.

Figure 7: Authentication Stage 7: A sends challenge to B

Stage 8. B now computes E_2 as shown below:

$$E_2 = 3DES_{K_{ENC}}(B \| Sig_{SK_B}[K_B \| B \| RND.A \| K_A])$$

The signature is a signature with message recovery, so all parameters in the signature can considered to be recoverable.

B now transmits E_2 and a MAC of the value E_2 to A, as shown in Figure 8.

Figure 8: Authentication Stage 8: authenticate B

A can now verify the MAC and decrypt E_2. Using the chain of certificates back to the root CA, A can verify the certificate from the IC manufacturer for B, which contains B's identify B and public key PK_B. Thus A knows, and can trust, B's public key PK_B. Hence A can now authenticate B by verification of the signature:

$$Sig_{SK_A}[K_A \| A \| RND.B \| K_B \| DH(g \| p \| q)]$$

At this point, the protocol is complete. A and B have a session key, have verified their respective identities, and have prevented replays. Any further communications, such as verification of biometrics, can now be carried out safely and securely.