

Privacy Increases Smart Card Security

By **Stefan Brands**
Senior Cryptographer
Zero-Knowledge Systems

Gus Hosein
Tutorial Fellow
The London School of Economics and Political Science

Stephanie Perrin
Chief Privacy Officer
Zero-Knowledge Systems

Structure

- 1.0 Introduction
- 2.0 Vulnerabilities of Smart cards
- 3.0 Containment of Privacy Risks
- 4.0 Privacy by Design
- 5.0 Implications

1.0 Introduction

Smart cards are a potential hazard to the privacy of the individual for several reasons. The cards themselves are not secure, being subject to tampering, duplication, and reading by hostile actors. The second problem arises from the infrastructure within which the cards are embedded, which facilitates data matching and collection. The third problem is the attractiveness of the cards, once the initial investment is made, to become de facto or explicit national identity cards, by combining all activities requiring a token to reside on the one card.

Other papers on this panel have concentrated on some of these issues, the focus of this paper is on the use of smart cards as tokens in a public key infrastructure, and more particularly, on the potential for a whole new paradigm for our thinking in terms of the utility and security of smart cards. The concept of private credentials which are cryptographically enabled and which provide irrefutable accountability and still do not permit the sharing of personal information or even require its collection and inspection, have been more thoroughly explained in Dr. Stefan Brands' white paper which we have also distributed at this conference, entitled *Private Credentials*.

The smart card systems currently in use rarely do anything to prevent organizations from linking and tracing all communications and transactions by the same cardholder. For security reasons, they operate by transmitting in each transaction a unique card identifier that can be linked to central database entries that hold all kinds of identifiable personal data. This enables organizations to compile extremely precise personal dossiers, containing detailed information about a person's financial situation, medical history, lifestyle, habits, preferences, whereabouts, and so on. The dossiers can be compiled, linked, and updated in real time without human intervention. Since smart cards shield their internal operations from their holder, it is virtually impossible to verify that a card does not leak personal data, its device identifier, its access control code, its communication and transaction history, data from other applications running on the same device, and so on. It is important to understand that even if nominative data is not stored or transmitted, the resulting profile linked to the identities

on the card can most likely be linked to the holder of the card. Certainly in legal investigations, the holder of the card would be hard pressed to deny ownership of the data trail.

Data protection principles accept smart card technology as being inherently invasive, and consequently try merely to contain the privacy problem that the technology leaves us with. As an example, consider how the UK Government framed its privacy concerns within its smart card consultation document [1]:

It is important that data-protection issues be considered from the outset of the introduction of any smart card scheme. ... The contractor shall implement procedures to ensure that information held on the smart card, and on any associated data processing or storage system, is accurate, current, and the minimum necessary for the purpose. When no longer required, information shall be purged from the card and associated systems.

The UK Government assumes that the "outset" refers to merely the discussion on how personal data is handled once gathered; the accumulation of personal data is considered to be the default.

Similarly, the US Government discussion paper on smart cards [2] equates smart card security and privacy of the cardholder in importance, but not in implementation. In discussing security, the Federal Card Services Task Force states:

Ensuring card security and cardholder privacy are of paramount importance. The government has committed to a rigorous security assurance program for smart card systems and operations. Electronic systems must be able to authenticate the user and other business partners so that only authorized personnel may gain access to restricted information, functions, and resources. [...] This plan calls for a smart card based extended ID authentication function to support multiple applications based on public key technology using the standard X.509 v.3 digital certificate and authentication framework as an operating model. [...] The government will continue to place strong emphasis on privacy rights for any data stored on government smart cards and/or card service systems. The government's security assurance program will remain focused on the integrity of data security and information privacy.

That is, the US Government plans to discuss how to deal with personal data once the security issues are met for implementing an ID-oriented multi-application smart card.

It is regrettable that after thirty years of discussion of data protection we still see a great deal of conflation of the concepts of security and privacy. Privacy is not confidentiality; it is a broader set of rights and includes informational self-determination. Security systems almost by definition are engineered to protect the interests of those who pay for them, and often these interests are not coincident with the security and privacy interests of the individual who is the data subject. These interests do converge significantly when the individual has rights of damages when his data has been abused, but we have not seen significant legal action in this area, nor assumption of liability by the card issuer. In fact, at least in North America, the reverse has held true.

Privacy advocates can no longer abdicate responsibility and blame the technology for forcing the abundant flow of identifiable personal data. We cannot simply wait for privacy invasive technologies to evolve and then demand that adequate privacy policies are followed, clamping a legal regime on to the technology after the fact. Privacy authorities are skilled at investigating breaches of data protection, and at analyzing dataflows and determining which instances of collection, use, and disclosure are justified and permissible in law, and which are not. This expertise must be brought to bear in the development of standards and technologies, because it is a rare technologist who is familiar with the lexicon of privacy protection. Adding privacy policies to ensure data protection once data has been gathered does nothing to address growing security risks from within and without an organization, from disgruntled employees, from hackers and industrial espionage artists, from hostile actors in civil litigation cases such as divorce liability and copyright infringement, and from ostensibly legitimate secondary users within the organizations themselves. Both public and private sector data users are under increasing economic pressure to use data more, to sell it to improve the bottom line, to analyse it intensively to minimize risk and ensure better returns on investment, to establish long-term customer relationships.

In this paper we argue that it is time for privacy commissioners and other privacy advocates to take a more active stance. Methods exist to design privacy into smart card/database infrastructures that meet the interests of all actors, including industry, government, and privacy advocates. In fact, as we will argue, by considering privacy as a design issue, everyone will have much less to worry about when it comes to security. We must insist on no less.

2.0 Vulnerabilities of Smart cards

Smart cards operate in environments where they interact with untrusted entities, such as their holders and card readers. Despite numerous claims from smart card developers and marketers that smart cards are secure, there is massive evidence suggesting otherwise.

One problem is that smart cards do not have their own display and keyboard. User identification data must be entered on a terminal communicating with the card, and this terminal must be trusted not to capture the user's identification data. Likewise, any results that the card wants to communicate to its holder must be displayed on the terminal. As a result, a variety of fake-terminal attacks become possible.

A more serious problem is that smart cards are not tamper-proof. Even though manufacturers work hard to improve smart card tamper-resistance, mass production smart cards will likely never be able to withstand physical attacks for more than a couple of years following their release. New sophisticated apparatus will appear, and existing apparatus is being improved all the time. Organized crime can hire expertise comparable to that in national laboratories, and sophisticated tools are increasingly becoming accessible to hackers and undergraduate students at technical universities. Often, sophisticated tools are not even necessary. The most powerful non-invasive attack is Differential Power Analysis, due to Kocher, Jaffe, and Jun[3], in which the attacker gathers information correlated to secret keys by using statistical analysis and error correction techniques. Invasive physical attacks require days or weeks in a specialized laboratory and are much more costly to undertake, but they are also much harder to protect against. Microprobe workstations and other sophisticated equipment can be used to physically damage a smart card chip in a controlled manner. Kommerling and Kuhn [4] "see no really effective short-term protection against carefully planned invasive tampering involving focused ion-beam tools."

A common trend has been to increase complexity through the idea of multiple applications for each smart card. That is, you can use the same smart card to gain access to your bank records as you can to purchase a coffee, while your medical records are stored in another part of the card. Multi-application smart cards introduce even more actors, and thus even more attackers. Also, the addition of complex circuitry and software can easily introduce new weaknesses in the tamper-resistance characteristics of the hardware. The ability to protect smart cards hinges on having enough capability and space for a software solution.

As Kocher, Jaffe, and Jun [3] point out with respect to Differential Power Analysis, the best way to deal with smart card vulnerability is to design cryptographic systems under the assumption that secret key information will leak. In light of this, one must operate under the assumption that smart card tamper-resistance is a matter of economics. At the very least, each smart card must have its own secret key. Also, to guarantee that a smart card design will be able to survive widespread physical compromise of smart cards, the design must provide for the ability to detect, trace and contain fraud if smart cards are compromised. Key and certificate revocation is well known as a difficult and costly problem both in smart card systems and in PKI architectures.

3.0 Containment of Privacy Risks

Three different levels of smart card identity disclosure can be discerned [5]. The first is impersonal smart cards, which lack identification; the personal data on the card need not be known by a third party. Examples are phone cards, non-personal customer cards, and pre-paid cards. The second type is the contractual pseudo-identification function, where the card is bound by contract to a particular person, but parties other than the card issuer do not learn the identity of the cardholder. The third type are smart cards with a general identification function intended for third parties, such as immigration, and driver licenses, implementing the

X.509 standard [6] on digital certificates. In this case, the third parties and the issuing bodies all know the identity of the card owner (and presumably sign this linking data between the card ID number and the X.509 certificate data), not only at the moment of card issue, but at any later transaction or other use of the card.

Just as the Social Security Number within the US and the Social Insurance Number in Canada have grown in usage beyond their original specifications, smart cards fall inevitably into the trap of scope creep. Smart cards quickly become multi-purpose, and could potentially act as universal ID cards. The inverse is that a card first begins as a national ID card with an X.509 digital certificate, and then multiple applications get added, where you can also use the card to gain access to government buildings and documentation; followed by additional uses under the first type of identity-disclosure, such as for use on the local transport system. Such a growth of applications seem to be justified by the increasing number of transactions with government today and the fact that repeating the costly building of an architecture of identification and card issuing is hard to justify in a government setting where taxpayers want costs cut. It is important to understand that building a reliable numbering system for identification of individuals is costly and labour intensive, it is far simpler to demand someone else's card (a driver's licence, a credit card, a social security card) than to go to all the bother of establishing an infrastructure yourself.

As the scope creep increases, additional problems arise. It is one thing to give your Social Security Number to your bank, but something completely different for it to be shared with your local video rental store because you choose to pay with your smart card. Data Protection advocates can intervene and demand that such numbers not be given to video rental shops or transport authorities, and rather some other unique identifier. However, we can be certain that pressure on such data collection and linkages will increase, until it will absorb a disproportionate amount of the time of Data Protection Authorities to police this.

The current architecture has drawbacks to industry as well. If it is the responsibility of a company to maintain the integrity and confidentiality of personal data, the costs and burdens of liability rise. Data that is kept is available for the purposes listed above, many totally unanticipated by the card holder, and the card issuers run the public relations risk of explaining to their customers what happens to their data, when a person is convicted in court because of data held that was generated by a card. Individuals do not yet have any appreciation of what data is generated in transactional datastreams, nor that it is kept and accessible for actions that could be hostile to their interests. Should the right stories start hitting the press, this could change overnight and presents a major public relations risk for companies not restricting data collection.

The disparity between perception and fact makes the smart card-only model extremely dangerous, especially since the interests of card issuers are not aligned with those of individuals.

4.0 Privacy by Design

This section discusses the possibility of re-introducing control over the flow of smart card data, by using the idea of Private Credentials. These allow card holders to decide how much information is actually disclosed, and to tailor the amount to each application. This addresses our privacy concerns, and at the same time brings resolution to the security concerns.

4.1 Private Credentials

Private Credentials enable individuals to determine for themselves when, how, and to what extent information about them is revealed to others, and to what extent others can link or trace this information. Private Credentials are discussed in greater detail in [7]. Here we briefly discuss the details as they pertain to the issues raised within this paper.

Digital certificates are traditionally a digitally signed document stating the name, personal data, and public key of the certificate owner. This document is signed by a Certificate Authority (CA), who binds the public key to the personal data. This certificate is then placed on the smart card and shared during transactions with third

parties, and which are authorised when the cardholder authenticates the certificate by use of a secret key, also kept on the card.

Private Credentials operate slightly differently. In this case, we still have a CA signing a binding between a public key, but this time instead of it being to an identity, the CA is binding a key and one or more attributes. An attribute is any type of information that is specified in a standard format. A Private Credential can specify any number of attributes. For instance, a “demographic” credential can specify its owner’s age, income, marital status, and residence, all neatly tied to a single public key, by means of one digital signature of the CA. The issuing protocol is performed in an interactive manner that ensures that the CA cannot learn the zeros and ones that make up the individual’s public key and the CA’s signature. That is, although these bit sequences are unique for each digital Private Credential that the CA issues, the CA obtains no information on who obtains which sequences. At the same time, the individual cannot prevent the CA from encoding the attributes into the Private Credential. An explanation of how these properties are achieved involves mathematics beyond the scope of this paper.

Private Credentials are much more powerful than paper-based certificates. For instance, each Private Credential holder can decide for him or herself, depending on the circumstances, which property to disclose of the data encoded into a digital Private Credential. This goes beyond the analogy of using a marking pen to cross out data fields on a paper-based certificate; a Private Credential holder can prove that he or she is either over 65 or under 18, for instance, without revealing which is the case.

Also, a Private Credential can be presented in such a manner that no evidence is left at all of the transaction; this is much like waving a passport when passing customs. Alternatively, it can be presented in such a manner that the only information left is self-authenticating evidence of a message or a part of the disclosed property; this is much like presenting a paper-based Private Credential with crossed-out data fields so that a photocopy can be made. Furthermore, the self-authenticating evidence can be limited to designated parties.

Furthermore, a Private Credential issuer can refresh a previously issued Private Credential without knowing the encoded data. The unknown encoded data can even be updated before it is recertified. By way of example, a doctor could issue a prescription to a patient for \$20 doses of a penicillin cure. Each time the patient visits a drugstore to collect some of the doses, the drugstore can verify that the patient is still eligible and can decrement the number of remaining penicillin doses. On the other hand, no drugstore can determine the total number of doses prescribed or the number remaining at the time of a visit, nor can different visits by the same patient be linked. The patient could even pay for each dose in untraceable electronic cash and receive a digital receipt that could be used to get reimbursed by his or her health insurance company.

Private Credentials even improve the privacy of organizations. An organization can verify a Private Credential in such a manner that it receives self-authenticating evidence that proves that the Private Credential has been shown but unconditionally hides all or an arbitrary part of the property that has been demonstrated. In applications where organizations submit the Private Credentials they receive to a central authority, to enable the latter to compute statistics or to combat fraud, this property prevents the central authority from learning which information an organization's customers disclosed.

4.2 Private Credentials and Smart Cards

Private Credentials can readily be implemented in smart cards. It is best to not use smart cards as stand-alone devices but in conjunction with user-controlled computing devices. This is the most natural setting in many communication and transaction settings. For example, a smart card can be used over the Internet only if it is connected to a desktop computer, notebook, handheld, a mobile phone, or some other device.

By routing all the communications from and to the smart card through a computer trusted by its user, the user’s computer can prevent the smart card from covertly sending out data, and can sift data before passing it on or halt a transmission in case data fields do not comply with protocol specifications. In addition, any data leakage by or to the smart card can be blocked. Furthermore, it can be assured that the smart card cannot learn the Private Credentials of its holder, the data encoded into the Private Credentials, or the properties disclosed

when showing a Private Credential. The cardholder can even prevent the smart card from developing random numbers and other information that would enable the issuer to trace the cardholder's transactions once it gains access to the card's contents. These properties hold in the strongest possible sense, namely in the presence of issuers that have access to cryptographic backdoors and conspire with Private Credential verifiers.

Even if all organizations (including those that issue Private Credentials and those that verify them) conspire and have unlimited computing resources, and issue smart cards programmed in adverse manners, they cannot learn more about honest Private Credential holders than the assertions they voluntarily demonstrate. Different actions by the same Private Credential holder cannot be linked, unless the Private Credential holder consents and cooperates.

This approach ensures that smart cards cannot be misused for the purpose of surveillance. At the same time, it offers important security advantages over the traditional approach. Firstly, since smart cardholders can enter their password, PIN, or biometric using the keyboard of their user-controlled computer, and can read messages on their computer's display, fake terminal attacks can easily be prevented. Secondly, most of the computational and storage burden of the smart card are moved to the user-controlled computer, which can be much more powerful; the extra space available can be used to improve tamper-resistance. Thirdly, Private Credentials greatly reduce the risk of identity fraud, simply because identity is not the basis for conducting transactions and communications. Fourthly, because Private Credentials can specify all the data that a verifier needs in order to decide whether to provide a service, the verifier does not need to consult central databases; this eliminates the security risks of central databases. Fifthly, the user's computer can safeguard the secret keys and other sensitive data of the user.

5.0 Implications

Privacy concerns are one of the main reasons why smart card implementations worldwide are stalling. As Schwartz[8] notes, "Ultimately, smart cards will not be able to succeed if consumers do not trust them. If the tracking ability of the cards weighs greater in the minds of consumers than convenience, the cards will not succeed in the market."

As privacy advocates we should not be content merely with managing the vast amounts of personal data gathered and stored by organizations. We must return the control to the individual, by letting the individual determine how much information may be released. We should reject entering into discussions that treat privacy and security as conflicting goals, and make the case that hardwiring privacy into the design of smart card systems actually enhances their security. With Private Credentials, smart card users can decide on a case-by-case basis how much and what kind of personal data is released.

It is worth noting here that, as with all major paradigm shifts, there is a lot of education that will be necessary in order to ensure acceptance of this approach. Auditors and all those accountable in organizations are accustomed to gathering personal information and transactional data to support accountability for the expenditure of funds, for the granting of benefits and the deployment of organization resources, and for law enforcement accountability. It is counterintuitive to not gather data, and there will be considerable resistance until the realities of public key cryptography and its potential to provide privacy are integrated into our thinking. Security specialists are among those most aware of the vulnerabilities of gathering data, and privacy experts ought to join common cause with them. Most countries are engaged in public discussions on the need for critical information infrastructure protection. Data Commissioners must insist that protection of personal information and its minimization is a fundamental pillar of the protection of the information infrastructure.

Private Credentials are not complementary to identity certificates, but encompass them as a special case. While we do not suggest to replace all identity certificate systems right here and now, it is important to bring the unbridled spread of privacy-invading smart card technologies to a halt. Privacy and security are not conflicting goals: they can reinforce one another, bringing benefits to everyone.

Endnotes

1. Information Age Government Champions, Her Majesty's Government Cabinet Office, Smart card Consultation, <http://www.iagchampions.gov.uk/iagc/guidelines/smartcards/privacy.htm>.
2. Federal Card Services Task Force, *Federal Smart Card Implementation Plan: The Future is in the Cards*, Electronic Processes Initiatives Committee, January 30, 1998.
3. Paul Kocher, Joshua Jaffe, and Benjamin Jun, *Introduction to Differential Power Analysis and Related Attacks*, Cryptography Research, 1998. Presented at CRYPTO '99. Document available at <http://link.springer.de/link/service/series/0558/papers/1666/16660388.pdf> , Abstract at: <http://link.springer.de/link/service/series/0558/bibs/1666/16660388.htm> LNCS 1666, p. 398 ff.
4. O. Kommerling and Markus G. Kuhn (1999). *Design Principles for Tamper-Resistant Smartcard Processors*, appeared in Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99), Chicago, Illinois, USA, May 10-11, 1999, USENIX Association, pp. 9-20, ISBN 1-880446-34-0.
5. Report of the Ministry of Justice Working Group (1998), *Social risks of smartcards*, January 1998; contributors are J.H.A.M. Grijpink (AJS), J. Henseler (GL), F.M.T.F. Hooghiemstra (KLPD), H. Kamp (DCB), R. van der Knijff (GL), G.J. de Raaf (DCB), W. Ruitenbeek (IND).
6. Austin Hill and Gus Hosein, *The Privacy Risks Of Public Key Infrastructures: Exposing The Dangers That Ubiquitous Digital Signatures And Public Key Infrastructures Pose To Individual Privacy, And Exploring Some Possible Solutions*, presented at the 1999 Data Protection Commissioners conference in Hong Kong, and available in draft form at <http://is.lse.ac.uk/staff/hosein/pkirisks.pdf>.
7. Stefan Brands, *Rethinking Public Key Infrastructures and Digital Certificates - Building in Privacy*, The MIT Press, August 2000.
8. Ari Schwartz, *Smart cards at the crossroads: Authenticator of privacy invader? At Home With Consumers*, 19(3), December 1998. Available at: <http://www.cdt.org/digsig/pres/>