Smart Identity Management system using Biometrics

Dr.Kashif Qureshi

Department Of Computer Science, tel: +966 (0)535598451,Jazan University, Jazan, Saudia

Srk1521@gmail.com

Prologue

The introduction of the electronic passport by governments around the world marks a major step in the use of biometrics. In fact, the electronic passport, or e-passport for short, combines the use of three important technologies for identification: biometrics, smartcards and radio frequency identification (RFID). Smartcards - increasingly often RFID-enabled - are already commonplace in our everyday lives, and the use of biometrics is expected to grow significantly. Apart from being a potential user of these technologies for e-government services, the government also plays an important role as facilitator and regulator of these technologies.

This chapter discusses the technologies of biometrics and (RFID-enabled) smartcards and their use in electronic passports, and reflects on the introduction of e-passports, and the surrounding issues regarding security and the shift in the balance of power between citizen and government. It concludes with a critical review from the privacy perspective.

Section-1

1 The Smartcard

A smart card, chip card, or integrated circuit card (ICC) is any pocket-sized card with embedded integrated circuits. Smart cards are made of plastic, generally polyvinyl chloride, but sometimes polyethylene terephthalate based polyesters, acrylonitrile butadiene styrene or polycarbonate.

Smart cards can provide identification, authentication, data storage and application processing.[1] Smart cards may provide strong security authentication for single sign-on (SSO) within large organizations.

Smartcards are the leading technology for authenticating users of computer systems whenever something more secure than passwords is needed. The most prominent applications of smartcards are bank or credit cards, and SIM cards in mobile phones. Digital pay TV systems also use smartcards to control access to transmissions. Many companies (and indeed governments) issue smartcards to their employees to log-on to computers, or access the computer network and on-line services. Smartcards, usually contactless ones, are widely used for physical access control to buildings. Contactless smartcards are also widely used for public transport systems, for instance as the Oyster card in London or the ov-chipkaart throughout the Netherlands.

Apart from serving as authentication token, another important application of smart- cards is

for digital signatures. Qualified electronic signatures, the strongest form of digital signature under European legislation (EC 1999; CEN 2004), have to be created by a so- called Secure-Signature-Creation Device (SSCD). This SSCD is a trustworthy device that stores the sensitive data (cryptographic keys) needed to create digital signatures and performs the computation of digital signatures. Currently, a smartcard is the obvious - in fact, essentially the only - choice for an SSCD.

Finally, apart from serving as authentication tokens or SSCDs, smartcards can also be used as secure carriers of information, or data safes. An example is the German *Gesundheit- skarte* that besides identity information contains essentials from the card holder's medical record.

Smartcards versus government

Governments have followed suit in issuing smartcards as authentication tokens to their employees, to selected professional groups, or to all citizens. For example, the US government issues PIV (Personal Identity Verification) smartcards to all government personnel to control physical access to buildings and access to computers and information services; the Dutch government issues smartcards to all its employees (the 'Rijkspas') and to all healthcare professionals (the 'UZI pas', for accessing electronic medical records); the French government issues smartcards to all residents (the 'Carte Vitale') to automate administration in the public health service.

Apart from using smartcards for its own digital services, a question is whether the government should not provide a digital identity to all citizens with a smartcard as associated authentication token for general use. Many countries already issue smartcards to citizens as national electronic ID cards, or eID cards. For an overview of national identity card schemes in the EU and a comparison of their privacy features see (ENISA 2009).

There are four main purposes for an eID card:

1. It may be used as an authentication token in the physical world, i.e. used for the same purpose as ID cards, driving licenses or passports have been used for in the past, but with the added functionality that it can be read electronically.
2. It may be used to create digital signatures, serving as a Secure-Signature-Creation Device (SSCD) for qualified electronic signatures.
3. It may be used as an authentication token in cyberspace.
4. It may be used for data encryption and decryption, for instance to enable confidential email exchange.

The third use is what is often called eID, in the narrow sense of the term. The e-passport, discussed in Section 5, only serves the first purpose - more specifically, proving your identity at border control. Some e-passports can create digital signatures, which allows authentication over the internet, as discussed in Section 4, but this is completely unintentional.

Section-2

2 Smartcard and RFID technology

This section discusses characteristics of smartcards, and RFID-enabled contactless smart- cards, and the security they can offer, when used in electronic passports or other applications.

2.1 Smartcards

A smartcard is a tiny computer, contained on a single chip. Traditionally these chips were embedded in a piece of plastic the size of a credit card, but over the years variations in form and appearance have been introduced. Apart from its small size, the prime characteristic of a smartcard is that it provides security: it offers protection against unauthorized reading or modification of data on the card. The software on the card can enforce restrictions on data being read or modified, for instance allowing certain operations only after a user has been authenticated by means of a PIN, or never letting confidential information, for instance cryptographic keys, to be read from the outside. A smartcard can provide protection to the information on the card even against someone who has physical access to the card. This means an organization can issue cards to users even if it does not trust these users, or does not trust them not to loose their cards.

All this makes smartcards radically different from more old-fashioned magnetic stripe cards, which offer no protection whatsoever to the data stored on the magnetic stripe. Magnetic stripe cards are easy to clone, which has led to skimming attacks, where criminals copy magnetic stripes and spy on people entering their PIN, to then use cloned cards to withdraw cash anywhere in the world. The huge rise in skimming attacks has led to many banks switching over to smartcards, typically so-called EMV cards implementing the standard developed by Europay, Mastercard and Visa. Compliance with EMV is also promoted by the European Payments Council, as part of the implementation of the Single Euro Payments Area. Replacing magnetic-stripe cards and handwritten signatures by smartcards and PINs might not be a security advantage for all parties involved, as the move may be accompanied with a shift in liability in case of fraud or disputes. In the UK, the introduction of EMV cards has lead to some public debate (Anderson et al. 2006), as customers are by default responsible for fraud committed with their smartcard and PINs, whereas they are less likely to be held accountable for fraud committed with old-fashioned credit cards and handwritten signatures.

Smartcards are the natural choice for secure storage of biometric information. The card can protect the information, it cannot easily be cloned, and even if a card is lost or stolen, the protection it provides remains in place. In the case of an e-passport implementing Extended Access Control, as discussed later, this means the biometric information cannot easily be read from a stolen passport. Also, if people are allowed to carry their own smartcard with their biometric information, this sensitive information is then under their own physical control.

Although card holders carry ‘their own’ smartcard with them, and control physical access to the cards, the card issuer usually retains legal ownership of the card and remains in complete control over the software and data on the card. In

other words, the issuer keeps complete 'logical' control over the card. So the balance of power is very much in favour of the card issuer rather than the card owner. This does not mean that the card issuer can access any data on the card; cards are (or should be) designed so that private keys and PIN codes on the card are inaccessible to the issuer.

When using biometrics for verification, an ideal solution would be to implement the entire biometric system on the smartcard, so that the matching of the biometric is done on the smartcard. The stored biometric information then never has to leave the smartcard. Prototypes of such cards have been made, even with on-card sensors to take fingerprints. Unfortunately, the processing power needed for this exceeds what is currently available on reasonably priced smartcards. So typically the smartcard only provides the biometric information to an external biometric system that does the job of matching.

The security that smartcards provide is not 100%. Using highly specialized techniques and equipment it may be possible to read or even modify the data on the smartcard in unwanted ways. In other words, smartcards are not *tamper-proof*, but only *tamper- resistant*. For instance, close observations of the tiny variations in the power usage of a smartcard may reveal cryptographic keys used on the card; shooting a laser beam at the chip may change a few bits of data, even though doing this in a controllable and meaningful way is extremely hard. Apart from such physical attacks, there may be bugs in the software on the card that can be exploited. Fortunately, the software on a smartcard is relatively simple, and the chance of such bugs is therefore a lot smaller than, say, for a PC operating system. However, as the software on smartcards grows in complexity, the chance of such software bugs will increase. Continued technological improvements and the ongoing arms race between new attacks and new countermeasures mean that a smartcard's security has a limited shelf-life. Cards that are a decade old should not be considered secure. This is an issue in setting the validity period for say e-passports, which some countries chose to reduce to 5 years.

The Terminal Problem

An important and fundamental limitation in the security that smartcards can provide is caused by the absence of a keyboard or a display on the smartcard. Because of this, the card holder cannot communicate with his smartcard without the help of some other device that does have a keyboard and display. In the case of a SIM card this device is the mobile phone; in the case of your bank card it is an ATM or card reader in a shop. This device has to be trusted to keep communication between the card holder and the smartcard confidential and not to change what it being communicated.

For example, if you type your PIN on some card reader to buy something with your credit card, you have to trust the display for the amount you are paying, and you have to trust the device not to secretly store or reveal your PIN in some way. Using your card in a mafia-operated shop could cause problems. Criminals have gone as far as installing completely bogus but convincing-looking ATMs in efforts to defraud people. Similarly, if you insert a smartcard in a PC to digitally sign some document, then a computer virus on your PC could change the document before it is signed, or simply sign something completely different than what is displayed on the screen. This security threat is why some banks provide customers with a smartcard reader with a small display and a keyboard for internet banking; using a smartcard reader hooked up to the PC and then using the standard keyboard and display would also be possible, but this introduces the risk of PC-borne attacks on internet banking.

More generally, securing the link between a computer system and the human user is a big problem. Paradoxically, we know how to secure the connection between computers (including

smartcards) hundred of miles apart, even if these communicate over completely untrusted communication channels such as the internet. Securing the last two feet from the computer to the human user is much harder. Biometrics could be used here to authenticate the human user to the system, but not the other way around! However, remote use of biometrics, say over the internet, is fraught with difficulties: the remote biometric system can be physically tampered with, and fake inputs can be spoofed, all without risk of detection.

2.2 RFID

Radio-frequency identification (RFID) is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. Some tags require no battery and are powered and read at short ranges via magnetic fields (electromagnetic induction). Others use a local power source and emit radio waves (electromagnetic radiation at radio frequencies). The tag contains electronically stored information which may be read from up to several meters away. Unlike a bar code, the tag does not need to be within line of sight of the reader and may be embedded in the tracked object.

RFID tags are used in many industries. An RFID tag attached to an automobile during production can be used to track its progress through the assembly line. Pharmaceuticals can be tracked through warehouses. Livestock and pets may have tags injected, allowing positive identification of the animal.

Since RFID tags can be attached to clothing, possessions, or even implanted within people, the possibility of reading personally-linked information without consent has raised privacy concerns.

Traditional smartcards have metal contacts which are used for the electronic communication. Increasingly, however, smartcards are *contactless*. The chip is then equipped with an antenna for communication using radio waves. This technology is called *RFID (Radio Frequency Identification)*. Contactless smartcards can be hard to recognize, as the chip and antenna can be embedded inside plastic or paper, as is the case in the e-passport, and cannot be seen from the outside.

RFID devices, also called RFID tags or transponders, come in different shapes and sizes. More importantly, different types of RFID devices vary considerably in the distance at which they can be activated, and in the computing power they have.

The RFID cards in e-passports are so-called *proximity cards*, which implement ISO 14443 standard. Proximity cards are widely used for access control to buildings and public transport. The typical operating distance for proximity cards is a few centimeters, but cards can operate at greater distances, using a larger and more powerful antenna in the reader, which raises obvious privacy concerns. Here it is important to distinguish between attacks where someone tries to activate a tag without the owner knowing, and attacks where someone only wants to eavesdrop on the communication when the tag is used with the owner's consent at a legitimate reader: the maximum distances for activation and for eavesdropping are different. For ISO 14443 proximity cards, remote activation has only been demonstrated at 27 cm (Hancke 2006) and theoretical predictions of what might be possible do not exceed 60 cm (Kfir and Wool 2005; TI 2003). Eavesdropping is possible at larger ranges: theoretically it is possible at up to 4 meters,

practically it has been demonstrated at 2.5 meters (BSI 2008). Note that the experiments above were done under carefully controlled circumstances, and will be hard to achieve in practice.

The simplest RFID tags do not have any computing power whatsoever, unlike the e-passport. All these tags can do is broadcast their unique serial number when activated, without any form of encryption. Such devices are commonly injected in domestic pets for identification and are set to replace optical bar codes in many application, as so-called Electronic Product Codes (EPCs).

Surprisingly, given the obvious risks to privacy, EPC tags are used in some identification documents: in the USA, they are used in the Washington State 'Enhanced' Driving Licenses

and in the Passport Card, a credit-card sized travel document for travel to Canada and Mexico. These RFID tags are very different from the proximity cards used in e-passports: they have a much greater range, and have been successfully activated from distances of 10 meters or more (Koscher et al. 2009), as opposed to 27 centimeters. Moreover, as these tags only broadcast some serial number, they can easily be cloned or spoofed, and allow easy tracking.

Section-3

3 e-Passports

A biometric passport, also known as an e-passport, ePassport or a digital passport, is a combined paper and electronic passport that contains biometric information that can be used to authenticate the identity of travelers. It uses contactless smart card technology, including a microprocessor chip (computer chip) and antenna (for both power to the chip and communication) embedded in the front or back cover, or center page, of the passport. Document and chip characteristics are documented in the International Civil Aviation Organization's (ICAO) Doc 9303.[1][2][3] The passport's critical information is both printed on the data page of the passport and stored in the chip. Public Key Infrastructure (PKI) is used to authenticate the data stored electronically in the passport chip making it expensive and difficult to forge when all security mechanisms are fully and correctly implemented.

The currently standardized biometrics used for this type of identification system are facial recognition, fingerprint recognition, and iris recognition. These were adopted after assessment of several different kinds of biometrics including retinal scan. The ICAO defines the biometric file formats and communication protocols to be used in passports. Only the digital image (usually in JPEG or JPEG2000 format) of each biometric feature is actually stored in the chip. The comparison of biometric features is performed outside the passport chip by electronic border control systems (e-borders). To store biometric data on the contactless chip, it includes a minimum of 32 kilobytes of EEPROM storage memory, and runs on an interface in accordance with the ISO/IEC 14443 international standard, amongst others. These standards intend interoperability between different countries and different manufacturers of passport books.

Some national identity cards (e.g. in the Netherlands, Albania and Brazil) are fully ICAO9303 compliant biometric travel documents. However others, such as the USA Passport card, are not.

Electronic passports - e-passports for short, also called biometric passports - have a contactless smartcard chip embedded in one of the passport pages.[1] From the outside, the only way to tell that a passport is an e-passport is by the logo on the passport cover. The e-passport chip stores a copy of the data written in the passport, such as name, date of birth, passport number, and expiry date. It also stores a digital copy of the passport photo, and possibly additional biometric data, such as fingerprint or iris information.

E-passports were introduced in the wake of the 9/11 attacks, when the United States government announced it would require passports to have embedded chips with biometric information in order to travel to the US under the Visa Waiver Program. However, in Europe discussion about of e-passports and use of biometrics was already underway earlier. (By the way, all 9/11 hijackers carried valid passports, and the requirement to carry valid *electronic* passports would have posed any additional obstacle in carrying out the attacks.) The International Civil Aviation Organization (ICAO), an agency of the United Nations, defined the international standard for the e-passports. The ICAO specifications still offers the freedom of various options, but guarantee basic interoperability of passports and inspection systems. Apart from facial images, the ICAO standards currently support the use of fingerprint and iris information as biometrics.

As an additional security measure, embedding chips in passports makes them harder to forge. However, as modern passports are reputedly hard to forge already, this does not seem to have been the main motivation for e-passports. Given that passports are hard to forge, much of the fraud with passports is through so-called *look-alike fraud,* where someone uses a real, but stolen or bought passport belonging to someone else who looks sufficiently similar. The facial images stored on the chip, which provide a higher resolution than a classic passport photo, could make look-alike fraud harder, as would any additional biometric information stored on an e-passport. The information could also be used to make it harder to obtain a passport in someone else's name, but only if the issuing organisation has records of previous applications. It is unknown how often such double applications occur.

The ICAO specifications (ICAO 2007) provide three security measures for the e-passports: Passive Authentication (PA), Active Authentication (AA), and Basic Access Control (BAC).

On top of this, the EU has adopted Extended Access Control (EAC) (BSI 2006) as an additional, stronger security mechanism for the fingerprint information in the second generation of e-passports, as this is considered more sensitive biometric information.

Both Passive Authentication and Active Authentication make it harder to make fake passports or tamper with a real one. Passive Authentication authenticates the data on the e-passport, by means of a digital signature over this data. This signature proves the data on the passport is authentic and has not been altered in any way. To verify the digital signature one needs the public key certificate of the issuing country. Passport inspection system have to be supplied with public key certificates of individual countries to be able to verify that the e-passport data carries the correct digital signature. Active Authentication authenticates the chip in the passport, by means of a challenge-response protocol, where the chip

---

Prior to the introduction of smartcards in passports, passports were already machine readable in the sense that the bottom of the main passport page, the so-called Machine Readable Zone (MRZ), can be automatically read using Optical Character Recognition (OCR) technology.

effectively digitally signs some random challenge sent to the chip. The chip carries its own public key certificate, signed by the issuing country, to provide that this signature is authentic. Passive Authentication is mandatory in the ICAO specifications, Active Authentication is optional. Although the e-passport is not intended for any on-line use, Active Authentication can be used for on-line authentication over the internet (van Dijk and Oostdijk 2009).

Accessing the passport chip

Basic Access Control (BAC) prevents access to the information on the passport chip without the user's consent. Because passport chips are contactless, an attacker could try to eavesdrop on the wireless communication between the e-passport and a legitimate passport terminal, say at border control at the airport. An attacker could also secretly activate the passport chip while it is in someone's bag or pocket and communicate with it by holding a reader close to it. These dangers would not exist with a contact chip, where the user must visibly give consent to anyone accessing it, by inserting it in a reader.[2] The main motivation for making the chip contactless has been convenience: contactless smartcards allow higher data rates, are less likely to fail because of dirt or wear and tear on the contacts, and are simply more convenient to use.

Some countries, including the USA, have introduced metallic shielding in the passport cover. Thin foil in the cover acts as a Faraday cage, making it impossible to activate the chip when the passport is closed. Note that this does not protect against eavesdropping, as the passport will have to be opened at passport control.

The (optional) mechanism of Basic Access Control provides protection against both eavesdropping and remote activation. With BAC, access to the chip is protected by an access code, preventing remote activation, and this access code is also used to encrypt communication between the e-passport and the terminal, preventing eavesdropping. The access code is part of the information that is written in the passport at the bottom of one of the passport pages, on the so-called Machine Readable Zone (MRZ). This information is optically readable, and is for instance used for automated check-in at some airports. The access code consists of the passport number, the date of birth of the passport holder, and the expiry date of the passport. Having the access code written in the passport may seem strange, but the basic idea makes sense: only as you hand someone your passport and thereby give them permission to open it and read it, do you give them access to the chip.

Drawbacks of the ICAO standards

A fundamental weakness of BAC is that, after eavesdropping on communication between e-passports and readers, an attacker can mount a brute force attack trying out all the possible keys. A proper password-based key exchange protocol would be better, and is in fact incorporated in Extended Access Control (EAC). This weakness in BAC is aggravated by the poor randomness of the access codes in the MRZ. At best, the total entropy in the MRZ is only 72 bits (Hoepman et al. 2006), which is less than current recommendations. If countries issue passport numbers in sequence, so that these are predictable and strongly correlated with the expiry date, this can reduce the search space substantially and make a brute force attack quite feasible.

Active Authentication (AA) prevents the cloning of passport chips by adding what is essentially digital signature functionality to the e-passport. The downside is that this way passport can be made to sign anything, by invoking the AA functionality, without the passport owner knowing.[3]

[2]Strictly speaking, the risk of eavesdropping still exists with a contact chip, but then the attacker has to physically tamper with the reader.

[3]Of course, AA is only possible after BAC.

Although the intention is that the passport inspection system just sends a random number to be signed, a system could sent a specific number with some meaning, for instance a coded string saying "passport nr 1234567X was at Heathrow airport on May 12, 2010". The data that the card will sign is only small (8 bytes), but this is enough to code up some meaningful information, say time + GPS data. The chip authentication procedure that is part of EAC completely avoids this possibility, by using a different method for authentication.

Extended Access Control (EAC) improves BAC by providing a key exchange protocol that is more resistant to off-line brute force attacks, and improves AA by providing a chip authentication protocol that does not suffer from the signature problem. EAC also adds the possibility for the passport to authenticate the terminal. This allows the e-passport to only release fingerprint or other sensitive biometric information if the terminal can provide a certificate, issued by the government of the country that issued the passport, giving the terminal the right to do so. Each country can decide which other countries have the right to read this data from their passport, and give these individual countries digital certificates allowing them to do this. This means that someone stealing a passport cannot access the sensitive biometrics on the passport chip, without stealing an official passport inspection system from customs, or at least the certificate it contains. Certificates of passport inspection systems will be short-lived, valid only 6 months, to reduce the impact of them being lost or stolen. All this requires a complex infrastructure to manage certificates. Countries will have to exchange digital certificates by diplomatic mail, and periodically update the certificates in all the passport inspection systems used throughout the country.

Tracking

BAC and EAC regulate access to the data stored on the passport chip, but do not address the possibility that the chip itself can be remotely recognised. As specified in the ISO 14443 standard, upon activation an RFID tag broadcasts some arbitrary number, a so-called UID, to begin the communication. On most RFID tags this UID is a *fixed* arbitrary number; this number can then be used to identify an individual passport. To prevent this, in passports a different, randomly generated number should be used as UID each time the chip is activated. Most countries now use such chips, but at least initially some passports with fixed UIDs have been issued.

Even if passport chips send out random UIDs, so that an individual passport can not be recognised, passports from different countries are likely to use different hardware and software, which are then likely to exhibit some observable differences in behaviour. Indeed, it turns out that passports from many countries can be distinguished automatically before BAC takes place (Richter et al. 2008). Only if countries buy e-passports from the same vendor, and use identical hardware and software, can this be ruled out.

Digitally signed passport data

The possibility of tracking people via their e-passport has attracted most attention in discussion of the risks of e-passports, but there are other, less spectacular, consequences.

The information on e-passports is digitally signed to prove its authenticity. A fundamental aspect of a digital signature as a means of authenticity is that it be stored and transferred. In the case of the biometric information protected by EAC, it means that if country A gives country B permission to read such biometric data from their citizen's passports, there is nothing to prevent country B from storing this data, with the digital signature, to use at some later time, or to pass on to some other country or party who did not get permission from country A to access the

information. Moreover, as the data is digitally signed, anyone who gets the data can still check the signature.

In essence, the passport chip does not just show a photograph and say that this is really the facial image of the passport holder, but it effectively hands over an infinite number of witness-signed copies of the photograph which the reader can (re)use and re-distribute at will. And whereas a photocopy of a passport page does not carry the same authority as the original, a digital copy of an e-passport's digitally signed data does.

More generally, digital signatures make information more valuable to potential users, both legitimate and illegitimate ones, and make loss or theft of the information more of a concern for the owner. There is a difference between my passport photo showing up on the internet or a digitally signed passport photo - digitally signed by the Dutch government to prove it's really me - ending up on the internet.

From a privacy point of view, a safer alternative to digitally signing the data would be to use a protocol which does establish authenticity of the data, but which does not provide transferable proofs of authenticity (Monnerat et al. 2007). Alternatively, one could authenticate the chip, for instance as is done in EAC, and then rely on authenticity of the chip to ensure that the (unsigned) data it provides is also authentic.

Function creep

Function creep is a very useful concept for understanding government and surveillance. When a new technology is introduced to do one thing (one function), and is later used for an entirely different thing, that's *function creep*. It often seems as though governments plan to bring in potentially unpopular technologies by exploiting function creep. It goes like this: the government wants to do X where X requires some new and expensive technology Y. Unfortunately for them, X is fairly unpopular and if everyone knows that they're spending money on Y in order to do X then there'll be a huge fuss about it in the papers. So what they do is invent a new and popular thing Z that also requires the technology Y. When they're building Y they say it's for Z, but all the time they have in the back of their mind that they'll introduce X later on.

Function creep is one reason why civil liberties campaigners are so worried about ID cards. The government plans to introduce them as a non-compulsory thing which will only be used in ways that are useful to most people, or for purposes that are popular (like being nasty to immigrants, or catching terrorists). It won't actually do those things effectively, but that doesn't matter because that's not what they're really for. It's really there to build a large database on everyone to make the job of the civil service and police that much easier, and it may also undergo function creep in the future to make it compulsory to have one, and maybe later than that to make it compulsory to always carry it, etc.

For the e-passport to work it is only required that someone's biometric data is stored in the chip of their passport, and nowhere else. However, once the authorities collect the data for the production of e-passports, there is the temptation to also store this information in a database. And once the information is stored, there will be temptation to use it for a growing list of applications, a phenomenon known as *function creep*. As a case in point, the Dutch government is setting up a central national database, and whereas originally this data was to be collected only to support the process of issuing passports, the scope has been widened to also use it for law enforcement. One may question whether the potential benefits warrant the infringement of privacy and civil liberties, or indeed whether the government should treat all its citizens as potential criminals. One may also question the usefulness of such a national database;

if the data is used for verification, e.g. to find a burglar after fingerprints have been found on a crime scene, a large database containing biometric data of huge numbers of law-abiding citizens might not be so useful, given that the chance of false matches increases with the size of the database. Innocent citizens with a similar fingerprint to some serious criminal might experience considerable nuisance. (Note that the false match rates for fingerprint recognition mentioned earlier concern high quality fingerprints taken under controlled circumstances, not partial or smudged fingerprints lifted from a crime scene.)

The highly *de*central storage of sensitive biometric data on individual passports is much harder for any attacker to abuse on a large scale than a central database, which could be hacked by outsiders, or abused by insiders. An attacker would need physical access to the actual passport to obtain its data and, if the passport implements Extended Access Control, the attacker would also have to steal a valid terminal certificate. In practice this means that only countries which have such terminal certificates can collect large amounts of sensitive biometric data, by harvesting it at border controls.

Lessons learnt

A serious shortcoming in the e-passport from a privacy perspective is that for fingerprints the raw biometrics - an image of the fingerprint - are used. Storing a template does not necessarily rule out the possibility of abuse by someone producing fake input to the sensors of a biometric system, but it would rule out someone abusing the information to fake fingerprints marks.

Looking back at the introduction of e-passports, it is clear that the original ICAO specifications could be substantially improved. As discussed, both BAC and AA were found to have weaknesses. Weaknesses can simply be that security measures can be improved: e.g., BAC provides some security, namely protection against eavesdropping, which could be improved, as is done in EAC. Weaknesses can also be that security is at odds with privacy. For example, AA provides extra security (protection against fake passport chips) at the expense of privacy (the threat of unwittingly putting digital signatures), which is avoided by EAC. PA provides extra security (protection against fake passport data) comes at the expense of privacy (the leaking of digitally signed data).

Apart from aspects that could be improved in the standards, some individual countries also slipped up with the introduction. Some countries, including the USA and Belgium, did not implement BAC in the first e-passports they produced. Several countries, including the UK and Belgium, issued passports with very little entropy (randomness) in the Machine- Readable Zones. Some countries issued e-passports with RFID chips that had a fixed, unique UID, so that passports can be tracked. Again, a more general lesson here seems to be that some time and reflection should be taken to avoid such mistakes.

Section-4

4 Privacy issues in using biometrics and smart cards

In access control one usually distinguishes three stages, namely:

- *identification*: saying who you are, for instance via a login name, bank account number, or social security number;
- *authentication*: proving who you are, for instance via a password or a PIN.
- *authorization*: establishing what someone is allowed to do.

We shall briefly review to what extent biometrics

may be useful in the first two of these stages. Authorization is a separate process that is in principle unrelated to the means of identification and authentication.

Biometrics is definitely useful for identification. A key aspect of any biometrics, irrespective of the type, is that it uniquely identifies a person via certain physical or behavioral characteristics. Of course, the biometrics may be spoofed, just like a login name may not be yours, but remember we are discussing identification, not authentication at this stage. Identification is only the first step towards authentication. Biometrics is useful and easy to use for identification simply because you always carry it along.

Is biometrics also useful for authentication? Proper authentication is important because it may not only give you certain (access) rights, but may also bind you to certain obligations. The latter is often called *non-repudiation* and implies that you cannot refute or deny certain actions that you have performed, like in signing a letter. Biometrics for authentication is much more problematic. It assumes that:

1. only you are the source of fresh biometric measurements;
2. freshness of such measurements can be recognized;
3. you provide input to these fresh measurements voluntarily and consciously.

Only if all three points hold convincingly, biometrics can be used to hold people accountable. But as mentioned in Section 3, breathing on a fingerprint reader may be enough to reactivate the previous measurement. This undermines all three points.

These three points are highly problematic. A database storing biometric information is a dangerous source of non-fresh measurements. Therefore it is essential that only abstract feature templates are stored so that the original measurement cannot be reconstructed. Ensuring this is beyond the control of the person supplying the fingerprint. Even if only templates are stored, upon each fresh measurement one runs the risk that the biometric device surreptitiously stores the measurement itself.

This issue becomes more and more urgent with the increasing number of biometric applications and the ensuing risk of interaction and interference. Suppose two stores A and B both use my fingerprints in a payment application, so that I do not need to carry my bank card and remember my PIN, but can simply pay by putting my finger on a biometric reader device. This may offer convenience, but it offers very little security: for instance an employee with access to A's database may spoof my fingerprint at shop B and pay on behalf of me. This shows that fingerprints, or any other form of biometrics, are unsuitable for non-repudiation. In fact, in a few years time all the countries that I travel to will store my fingerprint, making it effectively useless for any security-sensitive form of authentication.

Certain high security facilities do use biometrics for access control. But they typically do not use it as their only form of access control and require some form of human supervision. Moreover, they use a relatively non-standard form, like hand palm or iris recognition, which is not used in many other places and are (therefore) more difficult to spoof. But clearly, if such forms become more widespread, their reliability decreases rapidly.

The conclusion is that biometrics may look convenient, but can essentially only be used for identification. It may be used as input for authentication - requiring an additional, different proof step, just like for a login name - but it should not be used as authentication itself. Being able to tell a social security number is also not a reliable proof of identity - even though it is sometimes accepted as such.

Privacy implications of biometrics

We identify several privacy concerns related to biometrics. First, as already mentioned, biometric measurements may contain much more information than is strictly needed for identification. This is most obvious with DNA, which contains a lot of information about your genetic build up - and of subsequent generations. Much of what is exactly contained in DNA is still poorly understood, but now already certain sensitive health risks may be visible.

Secondly, when improperly stored - as original measurements and not as abstract templates - biometrics may actually increase the risk of identity fraud. When a biometric database becomes compromised, or in the worst case becomes public, for instance via hacking or negligence, the stored measurements may be used for false authentications. This assumes that use of biometrics for authentication will continue, despite its unsuitability.

Thirdly, biometric information may be used for tracing people, either openly, for instance via public security cameras, or covertly. Tracing is primarily based on identification, not on authentication. Such tracing is based on biometric identification and assumes an already established database of measurements for look-up. National databases of fingerprints that several countries (including the Netherlands) are now building may be used for such purposes. They lead to a shift in the balance of power between state and citizens, as with such databases the state can identify people against their will.

Use of smart cards

Smart cards serve as credit or ATM cards, fuel cards, mobile phone SIMs, authorization cards for pay television, household utility pre-payment cards, high-security identification and access-control cards, and public transport and public phone payment cards.

Smart cards may also be used as electronic wallets. The smart card chip can be "loaded" with funds to pay parking meters, vending machines or merchants. Cryptographic protocols protect the exchange of money between the smart card and the machine. No connection to the a bank is needed. The holder of the card may use it even if not the owner. Examples are Proton, Geldkarte, Chipknip and Moneo. The German Geldkarte is also used to validate customer age at vending machines for cigarettes.

Main articles: Contactless smart card and Credit card

These are the best known payment cards (classic plastic card):

- Visa: Visa Contactless, Quick VSDC, "qVSDC", Visa Wave, MSD, payWave
- MasterCard: Pay Pass Magstripe, Pay Pass MChip
- American Express: Express Pay
- Discover: Zip

Roll-outs started in 2005 in USA. Asia and Europe followed in 2006. Contactless (non PIN) transactions cover a payment range of ~$5–50. There is anISO/IEC 14443 PayPass implementation. Some, but not all PayPass implementations conform to EMV.

Non-EMV cards work like magnetic stripe cards. This is common in the U.S. (PayPass Magstripe and VISA MSD). The cards do not hold or maintain the account balance. All payment passes without a PIN, usually in off-line mode. The security of such a transaction is no greater than with a magnetic stripe card transaction.

EMV cards can have either contact or contactless interfaces. They work as if they were a normal EMV card with a contact interface. Via the contactless interface they work somewhat differently, in that the card commands enabled

improved features such as lower power and shorter transaction times.

Are smartcards Big Brother's little helper (as phrased in Brands (2000)) or can they empower people? Actually both, but the emphasis in current deployment is more on the former than on the latter. Smartcards are most often forced upon people together with the obligation to use them on many occasions to authenticate themselves. Via such applications people leave traces and become less anonymous. Moreover, each authentication obligation may involve the transfer of personal information stored on the card, as in the case of e-passports. This traceability may happen in a subtle, unconscious manner, when wireless smart cards use fixed UIDs that they reveal every time they enter into the magnetic field of a card reader, see Section 5.

An essential aspect of (informational) privacy is being able to control access to one's own personal information, and keeping such information segmented in different spheres and roles in one's life. Smartcards may actually be useful for such purposes, because they provide secure storage of a limited amount of data and, more importantly, of personal cryptographic keys. With these keys one can encrypt personal data, so that local, in context storage is no longer essential: as long as I control the keys that are required for decrypting my information I don't care very much where this (encrypted) information actually resides "in the cloud".

More advanced modern smartcards have substantial computing power that allows them to perform non-trivial cryptographic operations which can be used for privacy friendly applications. A clear example is provided by anonymous digital cash, as originally proposed by David Chaum (Chaum 1985; Chaum et al. 1988). There is more recent interest in privacy-friendly protocols for attribute-based authorisation, like in Brands (2000). Access to many situations is based on possession of proper attributes, like having a valid ticket for entering a bus or a train, or being over 18 for buying alcohol. Such attributes need not involve an identity. But when your entire eID is read electronically at a liquor shop when you only need to show that you're over 18, there is an obvious overkill. It can lead to many forms of unwanted profiling or even to identity fraud. Similarly, with the introduction of smart cards for e-ticketing in public transport a (silent) transition has taken place from attribute-based to identity-based authorisation. Research is going on to make modern selective disclosure protocols run on advanced smartcards, see e.g. Batina et al. (2010) and the references therein, so that upon entering a train or bus a card can for instance securely demonstrate that it is a valid month card, without revealing its (card or owner) identity.

References

1. Anderson, R., Bond, M., and Murdoch, S. (2006). Chip and spin. *Computer Security Journal,* 22(4):1-6. See also http://www.chipsandspin.co.uk.

2. Batina, L., Hoepman, J.-H., Jacobs, B., Mostowski, W., and Vullers, P. (2010). Developing efficient blinded attribute certificates on smart cards via pairings. In Gollmann, D. and Lanet, J.-L., editors, *Smart Card Research and Advanced Application Conference (CARDIS 2010),* number 6035 in Lecture Notes in Computer Science. Springer, Berlin.

3. *Brands, S. (2000). Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT. Freely available via* www.credentica.com.

4. BSI (2006). Advanced Security

Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC). Technical Report TR-03110, Federal Office for Information Security (BSI).

5. BSI (2008). Messung de Abstrahleigenschaften von RFID-Systemen (MARS), Specifications. 1: Teilbericht zu den Moglichkeiten des passiven Mitlesens einer RFID-Kommunikation. Technical report, Federal Office for Information Security (BSI).

6. CEN (2004). Guide on the use of electronic signatures - part 1: Legal and technical aspects. Available from http://www.cen.eu.

7. Chaum, D. (1985). Blind signatures for untraceable payments. In Chaum, D., Rivest, R. L., and Sherman, A. T., editors, *Advances in Cryptology: Proceedings of Crypto'82,* pages 199-203. Plenum Press, New York.

8. Chaum, D., Fiat, A., and Naor, M. (1988). Untraceable electronic cash. In Goldwasser, S., editor, *CRYPTO 1988,* number 403 in Lecture Notes in Computer Science, pages 319-327. Springer, Berlin.

9. EC (1999). Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures.

10. ENISA (2009). Privacy Features of European eID Card Specifications. Technical report, European Network and Information Security Agency (ENISA).

11. Hancke, G. (2006). Practical attacks on proximity identification systems. In *IEEE Symposium on Security and Privacy (S&P'06)*. IEEE.

12. Hoepman, J.-H., Hubbers, E., Jacobs, B., Oostdijk, M., and Schreur, R. W. (2006). Crossing borders: security and privacy issues of the European e-passport. In *IWSEC 2006: Advances in Information and Computer Security*, number 4266 in Lecture Notes in Computer Science, pages 152-167. Springer.

13. ICAO (2007). Supplement to Doc 9303, Version 6 (Final). Technical report, ICAO. Available from http://mrtd.icao.int.

14. Kfir, Z. and Wool, A. (2005). Picking virtual pockets using relay attacks on contactless smartcard systems. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*. IEEE.

15. Koscher, K., Juels, A., Kohno, T., and Brajkovic, V. (2009). EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond. In *ACM Conference on Computer and Communications Security,* pages 33-42. ACM.

16. MBKZ (2005). Evaluatierapport biometrieproef 2b or not 2b. Technical report, Ministry of the Interior and Kingdom Relations.

17. Monnerat, J., Vaudenay, S., and Vuagnoux, M. (2007). About machine-readable travel documents privacy enhancement using (weakly) non-transferable data authentication.

In *RFID Security*.

18. Richter, H., Mostowski, W., and Poll, E. (2008). Fingerprinting passports. In *NLUUG Spring Conference on Security,* pages 21-30.
19. Thalheim, L., Krissler, J., and Ziegler, P.-M. (2002). Korperkontrolle - biometrische zugangssicherungen auf die probe gestellt. *C't magazin,* page 114. English translation, entitled "Body Check: Biometrics Defeated", by R.W. Smith available at http://www.extremetech.cOm/article2/0, 2845,13919,00.asp.
20. TI (2003). Radio frequency identification systems HF antenna design notes. Technical Report 11-08-26-003, Texas Instruments.
21. van der Putte, T. and Keuning, J. (2000). Biometrical fingerprint recognition: Don't get your fingers burned. In Domingo-Ferrer, J., Chan, D., and Watson, A., editors, *Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications (CARDIS 2000),* volume 180 of *IFIP Conference Proceedings,* pages 289306. Kluwer.
22. van Dijk, D.-J. and Oostdijk, M. (2009). Using the ePassport for online authentication. Technical Report TI/RS/2009/002, Telematica Institute.
23. Wilson, C., Garris, M., and Watson, C. (2004). Matching performance for the US-VISIT IDENT system using flat fingerprints. Technical Report NISTIR 7110, National Institute of Standards and Technology (NIST).
24. www.wikipedia.com