About Machine-Readable Travel Documents

Privacy Enhancement Using (Weakly) Non-Transferable Data Authentication

Jean Monnerat[1]⋆, Serge Vaudenay[2], and Martin Vuagnoux[2]

[1] UCSD, San Diego CA, USA
[2] EPFL, Lausanne, Switzerland
http://lasecwww.epfl.ch

Abstract. Passports are now equipped with RFID chips that contain private information, biometric data, and a digital signature by issuing authorities. We review most of applicable security and privacy issues. We argue that the main privacy issue is not unauthorized access through radio channel or data skimming as claimed before, but rather the leakage of a digital signature by government authorities for private data. To fix this, we rather need the e-passport to prove the knowledge of a valid signature in a non-transferable way. Besides, several identification protocols such as GPS identification in RFID could lead to challenge semantics attacks that are privacy threats. To fix this, we also need some kind of non-transferability.
In 2003, Steinfeld et al. proposed the universal designated-verifier signature (UDVS) primitive. Its drawback is in demanding verifiers to have public keys authenticated by the passport. One compromise was proposed by Baek et al. with the UDVSP primitive. We show that UDVSP does not provide non-transferability and fix it by using zero-knowledge proof of knowledge. We propose a simple method to protect Σ-protocols against offline Mafia fraud and challenge semantics. We apply this by proposing a simple protocol based on Guillou-Quisquater identification that only requires two RSA computations and would substantially enhance the privacy of the e-passport bearer.

1 Introduction

So far, the travel documents we are familiar with are based on low technology: hard-to-copy/forge printed paper with an ID picture. The UN International Civil Aviation Organization (ICAO) has been working on making them machine readable since 1968. There is now a discrete machine-readable zone (MRZ) which can be optically scanned by a machine. This MRZ contains little information and is mostly aimed at speeding up inspection at border controls. Since 1980, ICAO works on adding more machine-readable information. In particular, biometrics would be used to have a more automatic and secure people identification protocol. The standard was released in 2004. As minimal requirements, Machine-Readable Travel Documents (MRTD) must provide a facial image, a digital copy of the MRZ, and to have them digitally signed by the issuing country. The preferred platform is a contactless IC chip based on RFID technology.

Obviously, the goal of this effort is to strengthen security at border controls. Of course, one danger would be that security officers rely too much on automatic identification and control. This would be counterproductive for security since passport copies of low quality with clones of IC chips would pass security control more easily. At the same time, the use of embedded digital biometric data opens the Pandora box and could threaten humankind: machines would trace people and humans would have to fight very hard against errors in databases or machine errors. For instance, the advent of video surveillance together with automatic face recognition jeopardizes the legitimate right to stay anonymous in a crowd. More dramatically, if criminal organizations can no longer steal identities without genuine fingers, they will start cutting fingers. This is what happened with biometric car lock systems.

⋆ Supported by a fellowship of the Swiss National Science Foundation, PBEL2–116915

Despite (and thanks to) privacy lobbies, the standard is now being deployed with facial image as the (only) biometric data. In addition to this, the EU has just extended this standard to accommodate fingerprint and iris images protected by a more secure access control protocol. In 2007, this extension is being implemented.

So far, researchers concentrated on demonstrating that unauthorized radio access to the chip and passive eavesdropping are feasible (although not technically straightforward). Our position is that the privacy threat coming from radio technology is not so important compared to having digital information released. In particular, having private information such as "official" name, gender and birth date digitally signed could be some valuable information which could be sold and threaten the privacy of people. People considering their age as the most sensitive private data would face to non-repudiable proof of it published in newspapers or put in databases. Transsexuals would also mind having a proof of there official gender released.

To solve this, we propose to use a cryptographic primitive that makes it possible to authenticate data without leaking any transferable proof. We build our primitive based on a zero-knowledge (with malicious verifier) proof of knowledge. Our aim is mainly to provide a proof of concept rather than a formal cryptographic study of a new primitive. For this reason, we do not aim at entering too much into the cryptographic technicality but rather to propose a concrete and easy protocol. Formal analysis will be subject of a subsequent study.

Previous work. The first research paper about the concept of e-passport by Davida and Desmedt [10,11] ages from 1988.

In [1], Avoine and Oechslin discussed information leakage from various communication layer protocols, including the singulation protocol for RFID. ISO 14443 recommends that RFID chips introduce themselves by using a random identification number that is used for collision avoidance only.

In 2005, Juels, Molnar and Wagner [27] presented a survey on MRTD and RFID. Among other issues, they discussed about the "biometric threat" and shortcomings in the Basic Access Control (BAC) protocol. In 2006, Hoepman et al. [23] discussed more about unauthorized access and skimming over the BAC protocol. They studied the entropy of the MRZ_info access key. They also discussed about the EU Extended Access Control (EAC). They detailed a revocation issue related to terminal authentication. They further discussed on biometrics. An experimental attack based on the BAC weaknesses was reported in 2006 by Hancke [22] and Carluccio et al. [6]. In 2006, Lehtonen et al. [28] studied ways to make optical memory and contactless IC chip interact for the benefit of security.

Non-transferability concerns were originally raised in the context of *undeniable signatures* [7] (also called *invisible signature*). The verification of such signatures is done interactively with the signer and should only convince the legitimate verifier. Later, the notion of *designated confirmer signature* of Chaum [8] allowed the invisible signature to be proven online by a designated third party called the *confirmer*. In order to cope with some attacks [13,24] allowing a malicious verifier to convince other non-legitimate parties, Jakobsson et al. [25] introduced some so-called *designated verifier signatures* which can only convince a designated verifier. As a price to pay, these techniques require the introduction of a pair of keys associated to the legitimate verifier. To the best of our knowledge, a formal (simulation-based) definition of the non-transferability was first proposed by Camenisch-Michels [5] for designated confirmer signatures. In the standard model, this definition (and subsequent variants) can be seen as a stronger (online) variant of black-box zero-knowledge against malicious verifiers.

Our contribution. In this paper we first survey the standards and reported security and privacy issues.[3] Our thesis is that research papers overlooked the main privacy threat: potential leakage of digital evidence. Finally, we discuss potential cryptographic solutions to replace digital signatures whose transferable property is a privacy issue. In between the extreme cases of traditional signatures (which are fully transferable) and of Universal Designated-Verifier Signature (UDVS) by Steinfeld et al. [34] (which are strongly non-transferable but require a heavy PKI on the verifier side), there is the proposal of UDVS Proof (UDVSP) by Baek et al. [2]. We show this does not achieve non-transferability. We propose a new protocol which *is* non-transferable after the protocol completed and does not require any public-key infrastructure on the verifier side. Our protocol can also nicely replace active authentication that also leaks.

2 The ICAO Standard

ICAO, the International Civil Aviation Organization, started to work on Machine-Readable Travel Documents (MRTD) in 1968. The first MRTD standard was issued in 1980. It proposes a standard Machine-Readable Zone (MRZ) consisting of two lines with basic information about the document holder. This MRZ is aimed at being read by an optical scanner. Basically, the MRZ contains: the document type (e.g. "passport"), the issuing country code, the holder name, the document number, the nationality of the holder, his date of birth, his gender, the expiry date of the document, and several options which are left up to the issuing country. Here is a (forged) example of MRZ for Mr Jean Dupont, born on April 1st 1973, citizen of France with a passport number 74HK8215 issued by Switzerland (is he a refugee?) expiring on May 12 2007:

```
PMFRADUPONT<<<<JEAN<<<<<<<<<<<<<<<<<<<<<<<<
74HK8215<6CHE7304017M0705121<<<<<<<<<<<<<<03
```

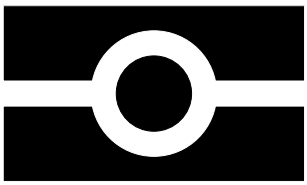
In 1980, the new-technology working group of ICAO started to work on biometrics. After 2001 9/11, the standardization process was boosted in order to have more security at the border control. In 2002, members decided to adopt facial recognition as the mandatory biometric and let finger and eye recognition as optional ones. The reason why they adopted face recognition is that giving a picture is already socially and culturally accepted by most of people worldwide. It is not intrusive, it does not require physical contact. Deployment is pretty easy. Enrolment is feasible from sample pictures and the holder (in particular: children) do not have to be present. Finally, human verification is still possible if the software crashes.

In 2003, members decided to focus on contactless IC chip as main support. The reason is that it requires no contact, unlike magnetic strip or contact IC chip. Furthermore, it offers large random access memory capacity compared to 2D barcodes. ICAO recommends to have at least 32KB memory and is pushing to 512KB so that many other applications can be installed.

Version 1 of the standard was issued in 2004. The technical part is detailed in two main documents: one about the Logical Data Structure (LDS) to be stored, the operating system, and the communication protocol to the IC chip [29], the other (called the *PKI Technical Document*) about the cryptographic aspects [30]. In this paper, we refer to these documents as the *ICAO standard*. These are technical reports that are aimed as being incorporated in future versions of *Document 9303*, the normative ICAO document about MRTD.

E-passports implementing the ICAO standard can be distinguished as they have the following logo printed on the cover:

[3] See [37] for a more complete survey.



The ICAO standard mandates the use of a digital picture (for facial recognition) and the MRZ as private information about the holder. It also mandates the use of PKI and digital signature to authenticate this digital information: this is the so-called *passive authentication*.

Several optional security protocols are offered by the ICAO standard.

- The so-called Basic Access Control (BAC) is used for reader access control and key agreement between the reader and the IC chip. A secure messaging protocol is then used for further communication. This protects the communication channel. The key agreement authenticates the reader to the IC chip based on the knowledge of the MRZ_info. This data is extracted from the MRZ. It consists of the document number, the date of birth and the expiry date (that is: the `74HK821` , `730401` and `070512` strings in our MRZ example). BAC is only based on the DES algorithm in encryption (2-key triple DES) and authentication (CBCMAC with a first key ended by a 2-key triple DES) mode. BAC is used to make sure that the reader has seen the MRZ, presumably by having the document given and opened by the holder for inspection. The goal of BAC is to prevent from unauthorized access and from passive eavesdropping (aka skimming).
- A so-called Extended Access Control (EAC) is left open to members by ICAO, but not standardized. Usage of EAC is up to bilateral agreements between members.
- The so-called Active Authentication (AA) is used to authenticate the chip to the reader. It uses public-key cryptography and proves that the chip is genuine. Namely, the public-key of the IC chip is authenticated as part of the passive authentication, and a challenge-response protocol proves that the chip holds a secret key related to the public key.

In addition to this, the IC chip must follow RFID standard ISO 14443. This means that it introduces itself by releasing an ID number to run a singulation protocol. To prevent from being traced, IC chips may use a random number.

The LDS document defines several LDS files called Data Groups (DG) from EF.DG1 to EF.DG19. Data group EF.DG1 is the digital version of the MRZ. Data group EF.DG2 is a facial digital picture which is optimized for automatic face recognition. These are the only mandatory data groups. Data group EF.DG15 is the public key of the chip if AA is implemented. Some other data groups can accommodate templates for digital fingerprint, iris image, written signature and other personal information (e.g. the place of birth, etc). Data groups EF.DG1 to EF.DG15 must be authenticated by means of passive authentication. To do so, the hash of all data groups is listed in an extra file EF.SOD called Security Object for the Document (SOD). This file also contains a formatted digital signature of this list. It can also contain the certificate of the Document Signer (DS) by the issuing country. If not present, this certificate can be obtained only from the ICAO public-key directory. Each country maintains its own PKI. It must send a self-signed certificate of its root certificate authority to all countries by diplomatic means, all certificates to the ICAO directory, and all certificate revocation list to all countries frequently or when needed. Data group EF.DG16 (which is not authenticated) contains the contact person to notify (presumably for the travel documents of children or persons requiring assistance). Other data groups are left for visiting countries to store electronic visa, automatic border clearance, or travel records.

Based on our own experiment and first-hand information, we have observed the e-passport characteristics on Table 1 for various countries. Note that characteristics can evolve in time. For instance, Belgian e-passports have switched from no BAC to BAC in 2006.

- As far as we know, only the USA use a metallic cover as a shield to the chip. This protects privacy (but rings at security gates).
- Following the ISO 14443B Part 3 standard, all RFID chips with random identifiers use a 32-bit number of format `08xxxxxx` . People deduce that an identifier starting with byte `08` means that the RFID chip is privacy sensitive and a potential target for adversaries. For that reasons, Australia decided to adopt a random 32-bit strings of arbitrary format. As a consequence, always changing identifiers not starting with `08` means that the RFID chip is likely to be the one of an Australian e-passport. As for US e-passports, we have heard contradicting first-hand information about whether they use a random identifier (like the Australian case) of a constant one. Thanks to the shield, using a constant identifier is a minor point though.
- Similarly, we have heard contradicting information regarding whether US e-passports use BAC or not.
- As far as we know, only Czech e-passports use active authentication.

So far, we have not seen any biometrics except facial images but this is likely to change pretty fast. Indeed, the Swiss government has announced in June 2007 that a new generation of e-passport with fingerprints will be released in 2009, conditioned to the Schengen agreements with Switzerland to be ratified by the EU. Presumably, all e-passports in the Schengen area will use EAC with fingerprints soon.

Table 1. Characteristics of E-Passports by Countries. (In boldface is what we have observed ourselves. Other information is first-hand information.)

	shield	singulation	BAC	AA
Switzerland	none	random `08xxxxxx`	used	not implemented
United Kingdom	none	random `08xxxxxx`	used	not implemented
France	none	random `08xxxxxx`	?	?
Australia	none	random xxxxxxxx	used	?
New Zealand	none	constant	used	?
USA	yes	?	?	?
Italy	?	constant	?	?
Belgium	none	?	used	implemented
Czech Republic	none	random `08xxxxxx`	used	implemented

Similarly, we had a look at public-key algorithms. We have 3 types of algorithms: the signing algorithm of the DS certificate; the signature algorithm of DS for the SOD; the signature algorithm in the active authentication. What we have seen is reported on Table 2. For instance, Switzerland uses ECDSA over P-256 (aka `secp256r1` [15,33]) to sign the SOD. P-256 has an order close to 2^{256}.

3 Security and Privacy Failures in the ICAO Standard

3.1 Radio Frequency Issues

So far, most of the academic effort to analyze the security of the ICAO standard concentrated on the consequences of having a contactless device. We review reported weaknesses here.

Table 2. Signature Algorithms (with signature length).

	certificate	SOD	AA
Switzerland	ecdsa_with_sha1 (824b)	ecdsa (512b)	n/a
United Kingdom	sha256withRSA (4096b)	RSA (2048b)	n/a
Czech Republic	rsaPSS (3072b) (using sha1)	RSA (2048b)	RSA (1024b)
Belgium	sha1withRSA (4096b)	RSA (2048b)	?
Germany	ecdsa_with_sha1 (560b)	ecdsa (464b)	n/a
Italy	sha1withRSA (4096b)	RSA (2048b)	?
New-Zealand	sha256withRSA (4096b)	RSA (2048b)	?
USA	sha256withRSA (4096b)	RSA (2048b)	?

Singulation. Some passports using a constant 32-bit RFID identifier (e.g. those from Italy or New-Zealand) can be tracked. Most of tested passports generate 32-bit random numbers starting with byte `08` for singulation as specified in ISO 14443B Part 3. As already mentioned, this can be used by adversary to identify the presence of an RFID with privacy enhancement which is likely to be an e-passport (at least some device having something to hide). Interestingly, Australia stepped out from the standard by deciding to start with a random byte instead. Clearly, this can further identify the presence of an Australian passport, the only RFID device behaving by announcing an ever changing random number not starting with byte `08`. We can thus trace people holding such a passport.

Privacy in RFID singulation is actually a big issue (see [1]). Even if an undistinguishable protocol is used, hardware always leaks due to radiation pattern signatures (see e.g. [21]). Ideally, *all* RFID devices should use the same hardware and follow the same protocol with the same implementation to avoid leakage, but this is clearly unrealistic.

Basic Access Control. BAC is the most documented security failure. Indeed, there is no free lunch. From an academic point of view, one-way primitives are not known to be sufficient to design any secure key agreement protocol [32]. When a key agreement based on weakly private information (such as MRZ_info) uses no public-key cryptography, it is vulnerable against online or offline bruteforce attacks. (See e.g. [27].) This is the same as for Bluetooth pairing [26,36].

The entropy of MRZ_info could ideally be of 70 bits (it contains a string of 9 alphanumerical characters, a date of birth with a 2-digit year, and a date of expiry for a document aimed at being valid for up to 10 years). In practice, it is much lower due to the passport numbering scheme which is being used by countries (see [23]). Hence, bruteforce attacks can be implemented as detailed in [6]. Based on that, online bruteforce attacks against a passport can be done. One experiment which took 4h was reported. One scenario where this kind of attack would make sense is during a long haul flight when an adversary wants to steal the private information of his neighbor. A passive adversary listening to the radio communication between a legitimate reader and the IC chip can also run an offline exhaustive search. In [22], the online attack was shown to be feasible at a distance of 1.5m while the offline attack was done a the longer distance of 4m. These attacks are further claimed to be feasible at a distance of 10m.

BAC was meant to protect against unauthorized access and skimming attacks. Our discussion shows that it does not complete its task.

Clearly, by replacing the key agreement protocol by the Diffie-Hellman protocol [14] or any other decent key agreement protocol, adversaries would no longer be able to decrypt private information by offline bruteforce. However, offline bruteforce would still reveal MRZ_info which is private as it contains a date of birth and a document number. To avoid that, a secure password-based authenticated key exchange protocol would be needed.

3.2 Other Privacy Issues

Although we believe that weaknesses due to the wireless link are real threats, we find that the impact of these problems is over-estimated compared to many privacy issues which are direct consequences of the overall philosophy of the ICAO standard. Indeed, unauthorized access or skimming is technologically hard to perform. Collecting data from authorized access to a document such as in a hotel check-in desk or in a duty free shop is much easier and threatening as detailed below.

Passive Authentication. The overall concept of passive authentication is a big loss for privacy. So far, data authentication is only based on a digital signature on private information. One problem with digital signatures is that they are transferable. Someone having access to the passport of someone else can not only get private information (what anybody would clearly assume) but also a proof of it. This proof can later be exhibited.

It is widely accepted to have to show a proof of identity, for instance at a hotel check-in desk, in department stores for duty free shopping, or at the cashier of a supermarket to buy some wine. A passport is a proof by itself. In hotels, it is further accepted that one copy of the passport will be kept. However, a copy of a passport is not a proof because it can easily be falsified. Hence, the passport holder can deny information based on this copy by claiming the copy was forged. People can thus continue to hide their age if they want to. Traditional passports are to some extend non-transferable proofs. With e-passports, the copy of the digital content with a certified signature is a transferable proof. Its semantic content can no longer be denied.

We believe that digital signature is clearly not the good way to authenticate data. To replace this, we propose to use some Zero-Knowledge (ZK) proof of knowledge of a valid signature. We could still have online transferability if the reader is playing the Mafia fraud attack (aka relay attack) [12]. To thwart this, one could even use more powerful non-transferable proofs but this would require a tedious public-key infrastructure for readers. Using ZK proofs at least ensures some kind of offline non-transferability. Such alternative protocols are discussed in Section 5.

Biometric templates in LDS. Disclosing biometric templates to help the reader to identify someone is also a big privacy threat. Contrarily to what people argue, disclosing the mandatory EF.DG2 file (the facial digital picture) is not the same as showing a small printed picture on the document. A first difference is that the digital picture is digital. As being such, it can be copied forever without any loss of quality. The second difference is that the picture is optimized for automatic face recognition. This means that a duty free shop can download the biometric picture and later install an automatic face surveillance control. A customer entering again would be automatically identified and his profile and previous shopping list would automatically appear to the vendor. This would indeed be a valuable information for the vendor willing to sell more.

As already documented, disclosing fingerprint templates is a privacy threat. The only way to avoid IC chips disclosing biometric information would be to implement on-board matching. The IC chip could identify its own holder. A challenging remaining problem would be to design a protocol that *proves* to the reader that the biometric templates did match.

Challenge semantics. The Active Authentication (AA) protocol basically consists, for the IC chip, in signing a random challenge provided by the reader. The signature is a proof of knowledge of the secret key that is attached to the public key that is itself authenticated from the LDS. Although pretty simple and secure from the perspective of the targeted MRTD functionality, this protocol has a quite surprising and terrible privacy problem as discussed in [35]. Indeed, the reader can put semantics in the challenge that will be gently signed by the IC chip. For instance, the challenge could consist of a

time-dependent social information at the time of the challenge (e.g. the current stock exchange rates, all collected press releases, etc) together with links to previous timestamps. Then a timestamp on the IC chip response would be a digital proof that the MRTD was examined at the given time.

An alternate solution for active authentication is already well known in the cryptography community since 1986: we can indeed use zero-knowledge identification such as the Fiat-Shamir protocol [16]. More recently, the GPS protocol [18] was shown to be pretty easy to implement on RFID devices [4,17]. This will be discussed in Section 5 as well.

4 The EU Extended Access Control

4.1 EAC Specifications

Pushed by privacy concerns related to biometric information, the EU has launched the development of a common Extended Access Control (EAC) to protect private data against unauthorized access. Despite our discussion from Section 3.2 about automatic surveillance abuse, it makes the distinction between "less-sensitive data" such as the MRZ and the facial image and "sensitive data" such as fingerprints. Nevertheless, the EU is likely to lobby for the ICAO to replace BAC by EAC in the future so even "less sensitive" data may benefit from this stronger protocol, eventually.

EAC accommodates a reader authentication based on an extra PKI. In clear, countries with bilateral agreements will be able to go through EAC (after having done BAC and checked mandatory face and MRZ data), to access to fingerprint and iris images. Countries without bilateral agreements will still be able to use BAC and get MRZ and facial image.

EAC is being implemented in 2007 based on the first version [35].

EAC consists of chip authentication and terminal authentication. Both must be used to treat sensitive private data. Terminal authentication must be used together with chip authentication. Chip authentication can be used alone, in particular as a possible replacement for AA as it prevents from the challenge semantics issues. In addition to this, chip authentication offers an extra key agreement (that is better than BAC) to be used for secure messaging. Chip authentication in EAC could thus replace BAC and AA at the same time and reach better security.

The PKI for terminals is similar as the PKI for MRTD except for the validity period which is much shorter. A certificate for a back-end terminal shall range between 1 day and 1 month. This protects against unauthorized access with stolen terminals. Unfortunately (as mentioned in [35]), the IC chip has no reliable clock. Hence, a stolen reader with expired certificate can still claim to have a valid one by giving an expired time. The chip could keep record of past given time to check that time is increasing, but this only protects frequent travelers.

Chip authentication is based on the Diffie-Hellman protocol [14]. It thus protects against passive skimming. The chip uses a static Diffie-Hellman public key while the reader shall use an ephemeral one. As the public key of the chip is authenticated by passive authentication, the key agreement is semi-authenticated in the sense that it authenticated the chip to the reader. The agreed key is later used in secure messaging. Note that chip authentication is implicit. It becomes explicit as the chip is later able to run secure messaging.

Terminal authentication follows the same principles as AA in a reversed way: the IC chip challenges the reader who gently signs the challenge. The challenge is signed together with the hash of the ephemeral Diffie-Hellman public key to authenticate the key agreement in the other way. Clearly, this can suffer from challenge semantics. The MRTD could get a proof that a given terminal did talk to the chip. It is claimed that readers are not concerned about privacy.

4.2 EAC Issues

Forward secrecy. Despite the claim that key agreement achieves forward secrecy, we obviously have a semi-forward secrecy: if the IC chip is corrupted so that the static Diffie-Hellman secret key leaks, communications can be decrypted.

Leakage of digests. Although EAC makes its best to protect sensitive data by a stronger access control, some content of the LDS can be recovered after BAC without passing EAC. Namely, the EF.SOD file is released after BAC. It contains the hashes of each data group, including sensitive ones. Hence, even though some fingerprint template is not released, the hash of it is given as a sketch. Since the terminal is likely to capture a probe that is likely to be close to the template, depending on the mutual information between the probe and the template, the sensitive template can be obtained by bruteforce.

Similarly, every data group for which the reader has a clue can be recovered. Obviously, this lacks semantic security: the reader can identify the right guess for sensitive data groups based on the EF.SOD data.

A quick dirty fix would consist in adding a random number in the sensitive data groups but it would be safer to think about using two levels of EF.SOD: one for less-sensitive data and one for sensitive ones.

Other issues. Finally, other problems such as offline bruteforce on MRZ_info in BAC, unauthorized download of MRZ and facial image based on MRZ_info, skimming of MRZ and facial image, possible leakage of transferable digital evidence, and possible leakage of biometric templates remain unsolved.

5 Non-Transferable Data Authentication

5.1 On Non-Transferable Proof of Signature Knowledge

The Mafia fraud [12] is an online transfer of an interactive proof that is a privacy threat. When an honest prover (the victim) must prove something to a verifier, the malicious verifier may try to transfer the proof to the Mafia. To do so, the verifier acts as a relay between the prover and the Mafia. To prevent from this attack, it is necessary that the prover authenticates the verifier and that the proof is dedicated to him. Techniques achieving this require the use of a public-key infrastructure on the verifier side. Verifiers are authenticated by proving that they hold a secret key attached to an authenticated public one. The key idea of non-transferable proofs consists of proving that either the statement is true or that the secret key of the verifier is known. Therefore, when the malicious verifier tries to transfer the proof to the Mafia this is no longer a proof of statement because it could have been forged with his secret key.

A Universal Designated-Verifier Signature (UDVS) was proposed by Steinfeld et al. [34]. Following this primitive, a signer (e.g. the document signer in the MRTD framework) can provide a signature to a prover (e.g. the IC chip of the MRTD). Then, the prover can prove his knowledge for a valid signature to any verifier with authenticated public key (e.g. the inspection device) in such a way that the proof cannot be transfered to anyone else.

The public-key requirement is a burden on the technology. One compromise would be to live with the Mafia fraud attack that is merely an online transfer proof but to make sure that no proof can be transfered when the protocol has been completed. This would define a weaker form of non-transferability but would be achievable without any PKI for verifiers. That is, the prover who participates to the proof protocol may prove a statement (in our case, the knowledge of a valid signature) to someone who may not be the person in front of him (or even to several persons) but is assured that the

statement cannot be proven by anyone else after the protocol is over. Namely, no proof can be posted in newspapers or stored as digital evidence.

Baek et al. [2] proposed an interactive UDVS Proof (UDVSP) with this objective in mind. One problem with their construction is that their security definition does not catch their objectives. Indeed, a malicious verifier following their proposed proof protocols could convert the interactive proof into a non-interactive one following the standard Fiat-Shamir techniques [16]. The proposed UDVSP schemes use Σ-protocols: protocols where the prover first sends a commitment, then the verifier sends a challenge selected in a pretty large set, and the prover responds so that the verifier can check whether the response is consistent with the document, commitment, and challenge. To convert the proof into a signature, the malicious verifier would use a random oracle fed with the document and commitment from the prover. Its output would initialize the random tape of the verifier. Then he would simulate the verifier algorithm and generate the challenge. The commitment and response would later become a universally verifiable signature of the document by having access to the random oracle. The verification scheme of the signature would simply consist in simulating the last step of the verifier with the given commitment and response. We can easily show that this signature is unforgeable if the challenge set is large enough. Indeed, no Σ-protocol can be ZK with a malicious verifier. (See [9].) We can best hope for honest-verifier ZK but this is not enough for non-transferability.

The problem in the [2] result is that they define their special form of non-transferability by the non-ability for an adversary to run the interactive proof again with a honest verifier. In our attack, the adversary does not run the interactive proof but convinces anyone for the validity of the signature by other means: a new verification algorithm. This does not contradict the [2] result but merely disprove that it offers any reasonable form of offline-transferability. Indeed, the definition of [2] for non-transferability is too weak. Here, we adopt a (weak) notion of non-transferability that comes for free with ZK proofs which are ZK with malicious verifiers: protocol transcripts using any verifier can be simulated so the proof gives no advantage to a malicious verifier.

When [2] was presented at Asiacrypt'05, Marc Girault made the comment that the proof of knowledge for an RSA signature [31] could easily be done using the Guillou-Quisquater (GQ) protocol [19,20]. Unfortunately, this could also be converted the same way since it is another Σ-protocol. Indeed, the GQ protocol is not known to be ZK. It is "only" known to be Honest-Verifier ZK (HVZK) and to resist impersonation under active and concurrent attack (see Bellare-Palacio [3]).

Protocols such as GPS [18] that could be used to replace AA are other (HVZK) Σ-protocols. Converting them into signature schemes could lead to other challenge semantics issues. To solve this issue, we propose to start Σ-protocols with a commitment from the verifier. The next section applies to the GQ and GPS protocols.

5.2 GQ-Based Proof of Signature and GPS-Based Identification

A fix to the GQ protocol would work as follows (see Figure 1). We assume that the prover holds an RSA signature x for a formated document digest X with public key (N,e) and secret key d. The prover wants to prove to the verifier his knowledge of x satisfying $x^e \bmod N = X$.

1. The verifier picks a random c_V of ℓ bits and commits to it by sending a commit value γ to the prover.
2. The prover picks a random y in $\mathbf{Z}_N^*$ and a random c_P of ℓ bits and sends $Y = y^e \bmod N$ and c_P to the verifier.
3. The verifier releases a decommit value δ to open c_V.
4. The prover opens the commitment and gets c_V then sends $z = yx^c \bmod N$ to the prover where $c = c_P \oplus c_V$.

5. The prover checks that $z^e \equiv YX^c \pmod{N}$.

A quick and dirty commitment would consist of picking a random string δ and committing by $\gamma = H(c_V, \delta)$ given a hash function H (ideally: a random oracle). The decommit value would be δ.

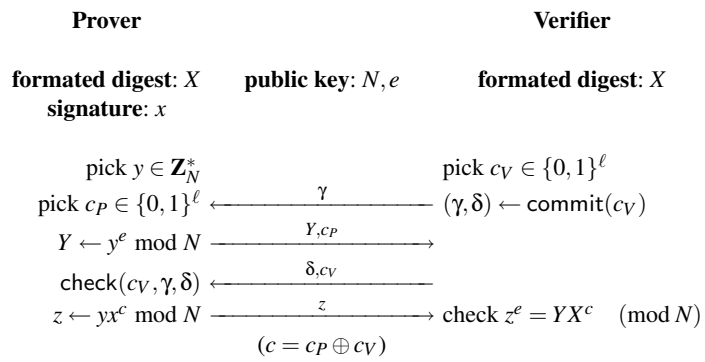


Fig. 1. A (Weakly) Non-Transferable Proof of Signature Knowledge based on GQ.

Unsurprisingly, when we use a binding commitment, we can prove that the protocol is ZK with malicious verifier by rewinding techniques. When we use a trapdoor commitment, we can prove that it remains a proof of knowledge.

Note that our protocol only involves two RSA computations on the prover side. Indeed, this would be similar as running two AA protocols on an MRTD.

To replace the AA protocol, we can simply use our proposed protocol with the message "I am the chip of [MRZ]". Owing a valid signature from the issuing authorities would assess the identity of the IC chip. This interactive proof would no longer be subject to challenge semantic issues as being (weakly) non-transferable. Another (more efficient) protocol would be based on GPS [18] (with a single iteration) as shown on Figure 2.

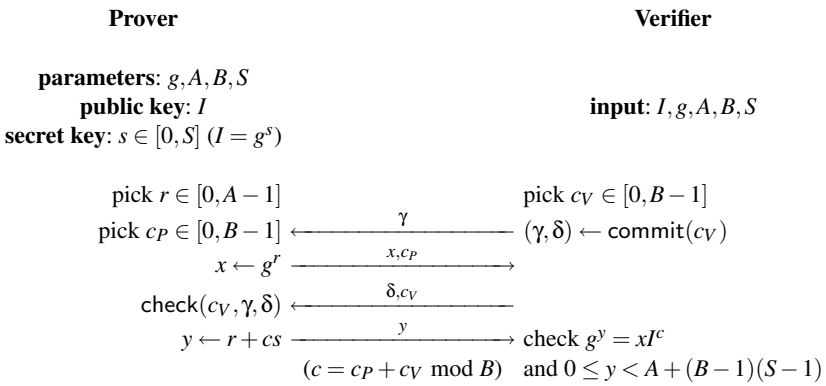


Fig. 2. A (Weakly) Non-Transferable Identification Proof based on GPS.

6 Conclusion

In this survey on machine-readable travel documents, we have reviewed most of security and privacy issues. Although the academic community mostly concentrated on unauthorized access form radio frequency or communication skimming, we believe that the main threats are in the release of digital evidence.

To solve the problem of passive authentication, we have proposed a scheme that makes it possible to prove that the LDS is authentic without leaking any evidence that could later be used.

The privacy issue in singulation is not as trivial as it looks and would certainly deserve a unique standard for RFID devices. If manufacturers adopt different standards, e-passports will always leak the radio signature of their manufacturer.

The release of biometric information is a privacy threat that demands to develop a new primitive: a proof of pattern matching that does not leak the original pattern.

Finally, we have shown several technical issues that would be easy to fix once spotted. Namely, BAC should be based on password-based authenticated key exchange as already mentioned in [27]. AA should be replaced by a real ZK proof, just like for passive authentication. EAC that is aimed at fixing the ICAO standard should stop leaking data group digests.

We hope that our result will contribute to reach a reasonable compromise between the security at border controls and the privacy of people.

Acknowledgments. We would like to thank all e-passport holders who kindly let us play with their private documents. We also thank those who gave us information: Justin Clarke, Martin Hlaváč, Thomáš Rosa, Adam Laurie, Gildas Avoine, and others. We started from Adam Laurie's tools[4].

References

1. G. Avoine, Ph. Oechslin. RFID Traceability: A Multilayer Problem. In *The 9th International Conference on Financial Cryptography (FC'05)*, Roseau, The Commonwealth of Dominica, Lecture Notes in Computer Science 3570, pp. 125–140, Springer-Verlag, 2005.
2. J. Baek, R. Safavi-Naini, W. Susilo. Universal Designated Verifier Signature Proof (or How to Efficiently Prove Knowledge of a Signature). In *Advances in Cryptology ASIACRYPT'05*, Chennai, India, Lecture Notes in Computer Science 3788, pp. 644–661, Springer-Verlag, 2005.
3. M. Bellare, A. Palacio. GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks. In *Advances in Cryptology CRYPTO'02*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 2442, pp. 162–177, Springer-Verlag, 2002.
4. B. Calmels, S. Canard, M. Girault, H. Sibert. Low-Cost Cryptography for Privacy in RFID Systems. In *Smart Card Research and Advanced Applications (CARDIS'06)*, Tarragona, Spain, Lecture Notes in Computer Science 3928, pp. 237–251, Springer-Verlag, 2006.
5. J. Camenisch, M. Michels. Confirmer Signature Schemes Secure against Adaptive Adversaries. In *Advances in Cryptology EUROCRYPT'00*, Brugge, Belgium, Lecture Notes in Computer Science 1807, pp. 243–258, Springer-Verlag, 2000.
6. D. Carluccio, K. Lemke-Rust, C. Paar, A.-R. Sadeghi. E-Passport: The Global Traceability or How to Feel Like an UPS Package. To appear in the proceedings of the RFID Security workshop 2006, LNCS.
7. D. Chaum, H. van Antwerpen. Undeniable Signatures. In *Advances in Cryptology CRYPTO'89*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 435, pp. 212–217, Springer-Verlag, 1990.
8. D. Chaum. Designated Confirmer Signatures. In *Advances in Cryptology EUROCRYPT'94*, Perugia, Italy, Lecture Notes in Computer Science 950, pp. 9–12, Springer-Verlag, 1995.
9. R. Cramer, I. Damgård, P. MacKenzie. Efficient Zero-Knowledge Proofs of Knowledge Without Intractability Assumptions. In *Public Key Cryptography'00*, Melbourne, Australia, Lecture Notes in Computer Science 1751, pp. 354–372, Springer-Verlag, 2000.

[4] available on http://www.rfidiot.org

10. G. Davida, Y. Desmedt. Passports and Visas Versus IDs. In *Advances in Cryptology EUROCRYPT'88*, Davos, Switzerland, Lecture Notes in Computer Science 330, pp. 183–188, Springer-Verlag, 1988.
11. G. Davida, Y. Desmedt. Passports and Visas Versus IDs. *Journal of Cryptology*, vol. 11, pp. 253–258, 1992.
12. Y. Desmedt. Major Security Problems with the Unforgeable (Feige)-Fiat-Shamir Proofs of Identity and How to Overcome Them. In *The 6th Worldwide Congress on Computer and Communications Security and Protection (Securicom'88)*, Paris, France, pp. 147–149, SEDEP, 1988.
13. Y. Desmedt, M. Yung. Weaknesses of Undeniable Signature Schemes. In *Advances in Cryptology EUROCRYPT'91*, Brighton, United Kingdom, Lecture Notes in Computer Science 547, pp. 205–220, Springer-Verlag, 1991.
14. W. Diffie, M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644–654, 1976.
15. Digital Signature Standard (DSS). *Federal Information Processing Standards* publication #186-2. U.S. Department of Commerce, National Institute of Standards and Technology, 2000.
16. A. Fiat, A. Shamir. How to Prove Yourself. In *Advances in Cryptology CRYPTO'86*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 263, pp. 186–194, Springer-Verlag, 1987.
17. M. Girault, D. Lefranc. Public Key Authentication with One (Online) Single Addition. In *Cryptographic Hardware and Embedded Systems CHES'04*, Worcester, MA, USA, Lecture Notes in Computer Science 3156, pp. 413–427, Springer-Verlag, 2004.
18. M. Girault, G. Poupard, J. Stern. On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order. *Journal of Cryptology*, vol. 19, pp. 463–487, 2006.
19. L. Guillou, J.-J. Quisquater. A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing both Transmission and Memory. In *Advances in Cryptology EUROCRYPT'88*, Davos, Switzerland, Lecture Notes in Computer Science 330, pp. 123–128, Springer-Verlag, 1988.
20. L. Guillou, J.-J. Quisquater. A "Paradoxical" Identity-Based Signature Scheme Resulting from Zero-Knowledge. In *Advances in Cryptology CRYPTO'88*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 403, pp. 216–231, Springer-Verlag, 1990.
21. J. Hall, M. Barbeau, E. Kranakis. Detecting Rogue Devices in Bluetooth Networks using Radio Frequency Fingerprinting. In *Proceedings of the Third IASTED International Conference on Communications and Computer Networks (CCN'06)*, Lima, Peru, pp. 108–113, IASTED/ACTA Press, 2006.
22. G.P. Hancke. Practical Attacks on Proximity Identification Systems (Short Paper). In *2006 IEEE Symposium on Security and Privacy (S&P'06)*, Berkeley, CA, USA, pp. 328–333, IEEE, 2006.
23. J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, R. Wichers Schreur. Crossing Borders: Security and Privacy Issues of the European e-Passport. In *Advances in Information and Computer Security, First International Workshop on Security (IWSEC'06)*, Kyoto, Japan, Lecture Notes in Computer Science 4266, pp. 152–167, Springer-Verlag, 2006.
24. M. Jakobsson. Blackmailing using Undeniable Signatures. In *Advances in Cryptology EUROCRYPT'94*, Perugia, Italy, Lecture Notes in Computer Science 950, pp. 425–427, Springer-Verlag, 1995.
25. M. Jakobsson, K. Sako, R. Impagliazzo. Designated Verifier Proofs and Their Applications. In *Advances in Cryptology EUROCRYPT'96*, Zaragoza, Spain, Lecture Notes in Computer Science 1070, pp. 143–154, Springer-Verlag, 1996.
26. M. Jakobsson, S. Wetzel. Security Weaknesses in Bluetooth. In *Topics in Cryptology (CT–RSA'01)*, San Francisco, California, USA, Lecture Notes in Computer Science 2020, pp. 176–191, Springer-Verlag, 2001.
27. A. Juels, D. Molnar, D. Wagner. Security and Privacy Issues in E-Passports. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05)*, Washington, DC, USA, pp. 74–88, IEEE, 2005.
28. M. Lehtonen, T. Staake, F. Michahelles, E. Fleisch. Strengthening the Security of Machine Readable Documents by Combining RFID and Optical Memory Devices. Presented at *Developing Ambient Intelligence: Proceedings of the First International Conference on Ambient Intelligence Development (Amid'06)*, 2006.
29. Machine Readable Travel Documents. Development of a Logical Data Structure — LDS For Optional Capacity Expansion Technologies. Version 1.7. International Civil Aviation Organization. 2004. http://www.icao.int/mrtd/download/technical.cfm
30. Machine Readable Travel Documents. PKI for Machine Readable Travel Documents offering ICC Read-Only Access. Version 1.1. International Civil Aviation Organization. 2004. http://www.icao.int/mrtd/download/technical.cfm
31. R.L. Rivest, A. Shamir and L.M. Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystem. *Communications of the ACM*, vol. 21, pp. 120–126, 1978.
32. S. Rudich. The Use of Interaction in Public Cryptosystems. In *Advances in Cryptology CRYPTO'91*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 576, pp. 242–251, Springer-Verlag, 1992.
33. SEC 2: Recommended Elliptic Curve Cryptography Domain Parameters. v1.0, Certicom Research, 2000. http://www.secg.org/

34. R. Steinfeld, L. Bull, H. Wang, J. Pieprzyk. Universal Designated-Verifier Signatures. In *Advances in Cryptology ASIACRYPT'03*, Taipei, Taiwan, Lecture Notes in Computer Science 2894, pp. 523–542, Springer-Verlag, 2003.
35. Technical Guidelines TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents — Extended Access Control (EAC). Version 1.01. Federal Ministry of the Interior. Bundesamt für Sicherheit in der Informationstechnik. 2006.
http://www.bsi.de/fachthem/epass/EACTR03110_v101.pdf
36. S. Vaudenay. On Bluetooth Repairing: Key Agreement based on Symmetric-Key Cryptography. Invited Talk. In *Information Security and Cryptology: First SKLOIS Conference, CISC'05*, Beijing, China, Lecture Notes in Computer Science 3822, pp. 1–9, Springer-Verlag, 2005.
37. S. Vaudenay, M. Vuagnoux. About Machine-Readable Travel Documents To appear in the *Journal of Physics*, 2007.