Resettable and Non-Transferable Chip Authentication for E-Passports

Carlo Blundo[2], Giuseppe Persiano[2], Ahmad-Reza Sadeghi[1], and Ivan Visconti[2]

[1] Horst Görtz Institute for IT Security, Ruhr-University Bochum, Germany
[2] Dipartimento di Informatica ed Applicazioni, University of Salerno, Italy

Abstract. Radio-Frequency Identification (RFID) is going to be the preferred technology for the realization of Machine Readable Travel Documents (MRTDs), and has been deployed in the last generation of e-passports. The proposed technical specifications for e-passport systems have been analyzed and criticized by security experts showing various functional, security and privacy deficiencies. The next generation of e-passports will implement more advanced cryptographic mechanisms, collectively known as Extended Access Control, and in particular a protocol referred to as Chip Authentication that protects an e-passport against cloning and transferability attacks. The Extended Access Control suite of protocols has found minor attention in the literature until now.
In this paper we point out possible attacks against Chip Authentication as proposed in the current specifications for Extended Access Control. In particular, we show that the possibility of transferability and reset attacks weaken the claimed security of the underlying Chip Authentication protocol. We also discuss the shortcomings of the existing literature on the security definitions for resettable identification protocols and propose a new definition that is more suited for real world scenarios. Based on known cryptographic techniques we finally propose an efficient protocol that is instead secure against such attacks.

1 Introduction

In an identification protocol a player P, called the prover, identifies herself to another player V, called the verifier. The main security requirement is to prevent an adversary from impersonating a player. One of the most serious attacks on an identification protocol is the so called *man-in-the-middle* attack where the adversary A plays two instances of the same protocol: in one instance A behaves like a verifier and in the other instance behaves like a prover interacting with a verifier trying to impersonate some other party.

Identification protocols are integral building blocks of various security critical applications. Depending on the application at hand one may require additional security properties beyond the sole goal of secure identification, and thus an identification protocol may be extended with additional cryptographic mechanisms. In this context, a prominent application with sophisticated security and privacy requirements is the *electronic passport* also called *e-passport* that we focus on in this paper as our use case.

The ICAO (International Civil Aviation Organization) has issued specifications for MRTDs (Machine Readable Travel Documents) [28, 25, 26, 15, 27, 23]. Many governments are developing new border control and visa systems that allow authorities to electronically access, store, retrieve, and transmit identification and biometric information about individuals. Radio-Frequency Identification (RFID) seems to be the preferred technology where the identifying information is stored on an RFID chip, embedded into the passport document, and retrieved using contactless reader devices (terminals) automatically and even unnoticeably.[3]

In Europe some countries, e.g., Germany, Belgium, and the Netherlands, have already started issuing electronic passports. The current implementations replicate the information contained in the paper passport. The next generation of e-passports will, however, store biometric information of the passport holder.

[3] Compared to video surveillance zones that require human post-processing of recorded data.

Other applications and features have been envisaged for the future, such as storing visa information on the chip [13].

Obviously the sensitive personal data stored on the RF-chip can be subject to various threats and must be protected to guarantee the confidentiality, integrity, and authenticity. However, since its appearance the e-passport initiative and the proposed schemes have been subject of diverse political and technical debates and criticisms. Advocates of MRTD systems envisaged horrifying threats by terrorist attacks and other criminal activities, claiming that e-passports enhance security, protect against forgery and manipulation of travel documents, identity theft, and speed up identification of individuals by allowing governments to build uniform data bases in standardized format [24]. On the other hand, privacy advocates are concerned regarding the security and privacy offered by the current specifications and particularly by the current implementation of e-passports. Many researchers and security experts have pointed out the security and privacy weaknesses of the deployed schemes (see, e.g., [17, 13]). Nevertheless, issuing states allowed a very fast roll-out of e-passports. [4]

In the following, we will motivate some important requirements to be fulfilled by identification protocols, in particular when deployed for very sensitive applications such as e-passport and examine whether the current enhanced proposal for e-passports, called *Extended Access Control* (EAC) ([18, 5] fulfills these requirements.

1.1 Requirements for Identification Protocols

We now discuss the core requirements for identification protocols, in particular we will stress the specific properties needed when an identification protocol is run by an RFID chip of an e-passport.

Non-transferability. An important security property of an identification scheme is that an adversarial verifier should not be able to exploit in any useful way the fact that a prover successfully proved his identity to her. In particular, we consider an adversarial verifier $\mathcal{A}$ that has taken part as a verifier in a successful execution of an identification protocol with prover P; then $\mathcal{A}$ should not be able to increase its chances of successfully completing an interaction with a third party D. In other words, $\mathcal{A}$ takes part in two distinct interactions: in the first $\mathcal{A}$ acts as a verifier of an identification protocol and in the second $\mathcal{A}$ interacts with a third party. We consider two forms of attack: off-line and on-line. In an off-line attack, the first interaction is executed in isolation and the second interaction starts after the first is completed. In an on-line attack, instead, the two interactions are executed concurrently. Notice that in the on-line attack it is always possible for $\mathcal{A}$ to relay messages from P to D. Such an attack by $\mathcal{A}$ is impossible to prevent unless some physical assumptions are considered in the system.

Fortunately, in the application of interest for this paper, on-line attacks are not practical as they require coordination between two executions and, solutions based on distance bounding [4, 6, 14, 32] would help to reduce/eliminate their viability.

Given the impossibility of achieving security against on-line man-in-the-middle attacks and the availability of ad-hoc physical solutions that prevent such attacks in the e-passport system, we will focus on off-line attacks.

[4] As mentioned in [9], the complexity of the system will be considerably increased: new cryptographic schemes must be deployed and new parties (e.g., chip and reader manufacturers, companies doing personalization of passports, service providers, Certification Authorities) are now involved, making the underlying trust model, trust assumptions, and trust relationships much more complex. Though an appropriate overall security evaluation of the realizations – especially concerning privacy aspects – has been either postponed or is made more difficult because of lack of public information.

Resettability (resilience to reset attacks). It is well known that the guarantee offered by standard security notions are void if the adversary has direct physical access to one of the parties – in particular when the adversary can reset the internal state of the party and make it run two instances of the same protocol using the same random coin tosses. Although physical capture is very unlikely for Internet security, small devices (like e-passports) can be rather easily captured and reset.

To model these attacks, Goldreich et al. [7] considered the concept of *resettability* for obtaining a security notion that is resilient to "reset attacks", e.g., attacks where the adversary can force a device to use the same randomness previously used. This notion has been then investigated in a sequence of papers [3, 21, 12] with the focus of achieving feasibility results and efficient constructions for zero-knowledge proofs (i.e., proofs where the verifier does not learn any information about the secrets) and identification schemes in such hostile settings. Reset attacks have been motivated in particular by the use of smart cards since some specific smart cards, when disconnected from their batteries, go back to their initial state and perform their computations using the same randomness they used initially. However, it is clear that the concept of a reset attack can have a wider applicability, in particular reset attacks are always possible when the adversary has control over the environment, and can therefore force a stateless device to use the same randomness in different executions of the protocols.

E-passports are often physically given to someone that wants to perform identity checks with them. Moreover, the random number generation of some RFID chips have already been successfully attacked due to their weak implementations. [5] The large use of e-passports therefore falls in the potentially threatening setting that we consider in this paper, and thus, it represents the main concrete attack that we study and want to prevent.

Practical setup assumptions. In many large scale applications, one desires practical setup assumptions and key management to avoid strong overhead. Solutions such as the framework of designated verifier proofs (see, e.g., [10, 16]) has been proposed for the purpose of having non-transferable protocols by relating the proof to the identity of the verifier (e.g., the prover proves that either he knows the claimed secret key or he has access to the verifier's secret key.). Hence, a cheating verifier attempting to transfer the proof to a third party will not be successful since he could have generated the proof by himself using his secret key. Unfortunately, such solutions require the existence and the deployment of a public-key infrastructure (PKI) for managing the keys of the verifiers. For e-passport, having a PKI on the verifier (reader) side is often an additional and strong overhead, since it is not practical to manage revocation lists and other updates.

Efficiency. Many of the settings where such identification protocols are employed, consider low-powered devices (smart cards, RFID chips) and thus there are important efficiency requirements concerning the round, communication, and computational complexities of the proposed protocols.

1.2 Our Results

In this work, we first discuss some important attacks related to the Chip Authentication protocol that has been included in the suite of protocols, called *Extended Access Control*, for the next generation of e-passports. In particular, we will show that the Chip Authentication protocol (see [18, 5]) is conceptually vulnerable to some off-line transferability attacks. We discuss the shortcomings of the security notions proposed in the literature for the identification protocols under the reset attacks. We then propose a new definition which refines the previous ones from which we believe to be more appropriate for real world scenarios. As a positive result, by building

[5] See, e.g., `http://www.hackaday.com/`.

on known cryptographic techniques, we will show an efficient, off-line non-transferable, resettable identification protocol that does not require a PKI on the verifier side.

Given the motivation of our work, our studies and results can be seen as a contribution to the design of secure identification protocols for scenarios, like e-passports, in which reset attack are to be taken into accounts. Note that electronic passports (or electronic identity cards) may be used as means for identification for many future security applications.

2 Background on Electronic Passport

The main cryptographic protection mechanisms of e-passport are: *Passive Authentication* (PA), *Basic Access Control* (BAC), and an *Active Authentication* (AA). Another authentication mechanism called *Chip Authentication* (CA) is proposed within the recent initiative of European Community for developing *Extended Access Control* based on [5].

PA shall guarantee authenticity and applies a digital signature to authenticate all relevant data stored on the MRTD chip. This signature is generated by a trusted Document Signer (e.g., the MRTD producer) in the personalization phase of the MRTD chip (see also [15]).

The function of BAC is to set up a secure channel between the reader device (part of the inspection system) and the e-passport that assures both confidentiality and integrity of the data communication. Note that both BAC and AA are optional mechanisms. BAC is already implemented, e.g., in Germany and the Netherlands. Current realizations of BAC deploy symmetric cryptography and generate the corresponding encryption and authentication keys from passport information through an optical interface, e.g., scanning the Machine Readable Zone (MRZ) which is visible in the physical passport document. As mentioned in introduction, meanwhile there is a relatively large body of literature on security and privacy weaknesses of the deployed schemes in e-passports (see, e.g., [17, 13]).

BAC has already been successfully attacked using offline dictionary attacks in the Netherlands due to the weaknesses in the passport numbering scheme [30]. Similar weaknesses are known for Germany [9] and Belgium [1]. Moreover, hardware-based machines, e.g., COPACOBANA (Cost-Optimized Parallel Code Breaker) [19] have been deployed to break BAC [20].

In [2], the authors have conducted an extensive investigation of the Belgian e-passport based on the ICAO specifications. Specifically, they showed that the effective entropy of the machine readable zone of the passport is only about 38 bits. In addition, in case an adversary has a targeted victim, it is realistic to assume that his date of birth is known (or can be approximated with a reasonable approximation). Since the date of birth is part of the machine readable zone, the entropy can be as low as 23 bits in which case the BAC (Basic Access Protocol) can be effectively broken by exhaustive search. The authors make several proposals to increase the security of the BAC Protocol. One proposal is to use random passport numbers; this will increase the entropy to 73 bit which is still insufficient. In addition to this, the MRZ contains optional 14 characters that can be filled with random bits thus making exhaustive search impractical.

These examples are good indications that the current BAC deployed in the field for a large number of passports can be seen as broken and the corresponding personal (image, name, birthday, etc.) user information can be considered as revealed. Moreover, we stress that the first generation e-passport will be in use for the next 10 years.

Active Authentication should prevent cloning by introducing a key pair unique to each chip: While the public key is authenticated through the PA, the corresponding private key is stored in secure memory and cannot be read out. The chip then proves knowledge of this private key by means of a challenge-response protocol: the MRTD chip signs a challenge randomly chosen by the reader which recognizes the MRTD chip as genuine. Although AA protects against cloning, it introduces a privacy threat known as *Challenge Semantic* [5]: In AA the reader challenges the chip

to sign a value which the reader is supposed to choose randomly according to the specification.[6] A manipulated reader, however, may tailor the challenge such that one can recognize it later obtaining a proof that the e-passport holder/owner has passed a certain border. In this context the Chip Authentication protocol proposed in EAC [5] seems to tackle this problem. In EAC the author argues informally that the corresponding mechanism is a *non-transferable* proof of knowledge since everyone can simulate the protocol.

2.1 Extended Access Control (EAC)

The proposed specification for Advanced Security Mechanisms for MRTD [5] considers two different access control mechanisms, depending on the degree of data sensitivity. On the one hand, less-sensitive data (e.g., the MRZ, the facial image, and other data that is relatively easy to acquire from other sources) is protected by Basic Access Control (BAC) which only verifies that the inspection system has physical access to the travel document by requiring the MRZ to be read by an optical interface. On the other hand highly sensitive data (e.g., fingerprints, iris scan, and other data that cannot be obtained easily from other sources at a large scale) must only be available to authorized inspection systems. Highly sensitive data is protected by the Extended Access Control (EAC) which additionally verifies that the inspection system is entitled to read this data. It seems that the European Union tends to motivate ICAO to replace BAC by EAC in the future so that less-sensitive data can be protected by stronger cryptography.

The main protocols in EAC are *Chip Authentication* and *Terminal Authentication*. Chip authentication (see also 1) provides a key agreement to be used for secure communication.[7] The procedure is as follows: At the border an e-passport holder presents her e-passport to the border control who scans the MRZ on the e-passport and then places the e-passport near an inspection terminal to fetch data from the chip. The e-passport and the terminal establish an encrypted communication channel by executing the Basic Access Control (BAC) protocol. Then the terminal and the e-passport perform a mandatory Chip Authentication followed by a Passive Authentication. Finally, a Terminal Authentication is performed by the chip challenging the reader who signs the challenge.

EAC security and privacy issues. Although EAC [5] offers an improved security over the first proposed solutions for e-passport identification and authentication, it still suffers from the problems of BAC as long as it relies on BAC for driving the session key required to access basic identifying information stored on the chip. Moreover, some EAC issues have been pointed out in [22]: EAC does not provide complete forward anonymity since it uses static keys in the key exchange protocol which, if revealed, allows an adversary to decrypt the communication. Further, the digest of some security critical information can be leaked. On the other hand, EAC considers the challenge semantic issue for the terminal (reader) authentication as less important claiming that terminal privacy is not an issue.

In the following, we focus on Extended Access Control (EAC) [5] and point out several observations regarding privacy and security related problems and shortcomings which we believe must be carefully considered in the design and implementation of an highly sensitive application such as e-passport. In particular, we consider the transferability and resettability problems which are severe threats against authentication/identification protocols based on proofs of knowledge [3] (i.e., if a prover can convince a verifier, then there is a polynomial time program, called extractor, that by accessing the prover outputs a valid witness).

[6] The signature is used for proving knowledge of the secret key that is attached to the public key which in turn is authenticated from the Logical Data Structure.

[7] Chip authentication in EAC could thus replace both, BAC and AA, to improve security.

P**'s identity:** $\mathtt{pk}_{chip}$.
P**'s private input:** $\mathtt{sk}_{chip}$ **and** par_{chip} **is some parameter.**
P**'s randomness: Use the Random Number Generator.**

P: send $\mathtt{pk}_{chip}$ and par_{chip} to V.
V: randomly generate an ephemeral key pair (sk', pk') using the same domain parameters and send pk' to P, and derive a new session key $K \leftarrow KA(sk', \mathtt{pk}_{chip}, par_{chip})$ using the key generation function $KA()$.
P: derive a new session key $K \leftarrow KA(\mathtt{sk}_{chip}, pk', par_{chip})$ using the key generation function $KA()$.

Fig. 1. Chip Authentication Protocol.

3 Security Notions

In this section we will review security notions for non-transferability against reset attacks proposed in [3] and introduce our strengthening.

Identification protocols secure against reset attacks. The study of identification protocols in presence of resetting adversary has been done in the work of Bellare et al. [3]. In that paper security with respect to off-line attacks is referred to as CR1 security, while security with respect to on-line attacks is referred to as CR2 security. We will now discuss these notions and our newly introduced notion CR+ that is stronger than CR1.

CR+ *security.* Our new notion captures security in the following scenario. We have an adversary $\mathcal{A}$ that interacts with multiple instances of protocol Π with honest provers that are all running on input pk and using the same public information crs. $\mathcal{A}$ is allowed to reset any of the instances to any state and we do not want $\mathcal{A}$ to gain enough information from this interaction to successfully complete an identification protocol Π' with an honest verifier on input pk. In this case we say that Π is CR+ secure with respect to Π'. In the CR1 notion of [3] the two phases do not overlap in time (the interactions with the honest provers are to be completed before the interaction with the honest verifier starts) and the adversary $\mathcal{A}$ was playing the same protocol with honest provers and the honest verifier[8].

We get a stronger notion of security by considering adversaries that have more power. Specifically, in CR+ we allow the adversary to start the interaction with the verifier; the adversary can suspend the interaction with the verifier and start a resetting attack with the provers; finally, the adversary can resume the interaction with the verifier. The CR+ notion of security is certainly not weaker of the CR1 notion of [3]. For instance, consider the CR1-secure construction of [3] in which the identity is a public key pk of a CCA2 encryption scheme. The verifier sends a challenge ciphertext c and the prover answers by sending back the plaintext m. The following attack shows that this construction is not CR+-secure: $\mathcal{A}$ interacts with the verifier V and tries to identify herself using public key pk and with the legitimate owner P of public key pk. $\mathcal{A}$ receives challenge c from V and puts the interaction with V on hold. Then $\mathcal{A}$ start the interaction with P and sends c to P to which P replies by sending m. At this point the interaction with P is terminated and $\mathcal{A}$ resumes the interaction with V by sending m to V. Notice that in the attack outlined above, the adversary $\mathcal{A}$ first interacts with V then with P and then with V and $\mathcal{A}$ does not need even to perform a reset attack. We stress that, similarly to the CR1 notion of [3], in CR+ we do not allow

[8] Obviously $\mathcal{A}$ could play with many verifiers but this would not add extra power since any succeeding adversary $\mathcal{A}$ that plays with many verifiers can be reduced to a succeeding adversary $\mathcal{A}'$ that plays with just one verifier, by simply emulating internally all other verifiers required by $\mathcal{A}$.

the adversary to interact with the provers and the verifier at the same time. Indeed, if this kind of attacks were allowed, then the adversary could simply relay messages between the honest prover and the honest verifier and no protocol can be secure against this attack. In [3] these stronger attacks where considered in the notion CR2, however, their CR2 secure protocols assume that each interaction uses a different session ID. We do not follow this approach since in practice nothing prevents the adversary from using the same ID in all protocols as it does in the simple attack where it copies all messages. Therefore, given that the adversary has an easy strategy to win, we simply observe that there is no possible defense against on-line man-in-the-middle attacks when they are mounted, and thus it is anyway necessary to resort to physical means to make sure that the adversary will not play protocols with other verifiers when it is also playing with a prover. In this context one may use some additional techniques such as distance bounding [4, 6, 14, 32] where one can guarantee that the protocol played by the prover with the man-in-the-middle will be executed in one shot, and it is isolated from the surrounding environment. Once we have this guarantee, we can focus on weaker and *achievable* security definitions.

In addition, there is another important improvement to CR1 that we consider in the definition of CR+. Indeed, we also allow the adversary $\mathcal{A}$ to play different identification protocols with the provers and with the verifiers. This covers the case in which one can design an identification protocol that can be successfully executed by an adversary (even without knowing the secret key) if an adversary has access to the prover of a different identification protocol. That is, in CR+ we allow $\Pi \neq \Pi'$ whereas in CR1 it was required that $\Pi = \Pi'$. The notion of [3] thus guarantees security only if the same public key was used in only one type of identification protocol. This is clearly difficult to guarantee in real-life scenario.

In Section 4 we give an identification protocol that is a proof of knowledge and is CR+ non-transferable with respect to *all* identification protocols that are proofs of knowledge.

Generalizing CR+ *to multiple access.* While it is reasonable to assume that by using some physical assumptions, one can be sure that the protocol executed by the prover is run in one shot, it is not immediately clear why the adversary should not be able to get access to prover's device in the future again, then again with the verifier and so on. Such extra power makes the attack of the adversary as strong as the CR2 attack, and thus it is impossible to obtain a secure identification protocol.

Indeed, observe that the restriction that the adversary plays with the provers in one shot, does not hold anymore as the adversary can then play some messages with the verifier and can later reset the prover. This concretely simulates the CR2 attack and allows the adversary to be a proxy that copies to the verifier all messages played with the prover. This extension of CR+ is therefore impossible to achieve.

An important question is therefore whether the extra power of the adversary in this extension of CR+ is always possible in real scenarios, and thus there is no reason to study CR+ anymore. However, consider the following example. Since the interaction with V is non-resetting, it does make sense to consider a scenario where the adversary suspends the execution with V, plays in one shot with P and then continues again the protocol with V. This makes sense because the interruption in practice can be just for a very short time and thus concrete timeouts of V do not expire. Instead the case in which the adversary plays again with the prover still maintaining the open connection with the verifier in some scenarios is not realistic. Indeed, consider the use of e-passports at the border control. The e-passport is used at the border control once and again at the same border control sometime later. So an adversary who obtains the e-passport at a border control could have already suspended a protocol with a verifier and could resume it a short time later, after having performed this (resetting) interaction with the e-passport. It is instead very problematic for the adversary to suspend again the protocol with the verifier and to obtain access to the *same* e-passport again since it will be used again by the same person at that border control after some longer time.

3.1 CR+ Transferability of Chip Authentication

We construct an offline man-in-the-middle (MiM) attack showing that Chip Authentication is not secure with respect to our notion of CR+-security. Consider the follow adversary $\mathcal{A}$ that first receives a message pk' that corresponds to a Diffie-Hellman (DH) contribution from an honest verifier V. Then $\mathcal{A}$ suspends the first protocol and it plays the Chip Authentication protocol with an honest prover P receiving the message m from P computed under the exchanged key (this message corresponds to the one required by passive authentication). Then $\mathcal{A}$ resumes the protocol with V giving back the identity of P and m to V who will be able to decrypt it. In this way V is convinced that he has interacted with P. This problem stems from the fact that $\mathcal{A}$ does not need to show that it knows the (exchanged) DH key before obtaining such a message from P.

Note that even though in the attack outlined above $\mathcal{A}$ copies messages between the two interactions the attack is offline.

4 Resettable Non-Transferable Identification

In this section we present an efficient identification protocol ID that considers the security issues previously discussed. We then analyze its security properties.

4.1 High-Level Overview

Before describing our contribution let us explain why previous approaches fall short of reaching our goal (CR+-secure identification protocols) and we start by considering the work of [22]. Here the authors present a secure identification protocol for the off-line setting (i.e., the man-in-the-middle does not work simultaneously with provers and verifier) and the protocol does not require PKI on the verifier's side. Indeed, the proposed protocol is a zero-knowledge proof of knowledge and as such it enjoys a satisfying security notion for both prover (i.e., the zero knowledge property) and verifier (i.e., the proof of knowledge property). Moreover the zero-knowledge property preserves the non-transferability of the protocol even in case the adversary will play with the verifier both before and after playing with the prover, i.e., in the setting obtained when using distance bounding on the prover side. The main weakness of the protocol proposed in [22] concerns the fact that they restrict the adversary to sequential interactions with the prover. This, however, as we have seen, is not realistic in some scenarios where the adversary has physical access to the device and can mount reset attacks against it. If one tries to strengthen the protocol of [22] to make it secure against concurrent/resetting adversaries, then the efficiency of their protocol is immediately lost (indeed, resettable zero-knowledge proof systems require at least a logarithmic number of rounds [8]). Moreover, there is no hope to preserve the proof of knowledge property (at least for the black-box sense) against a resetting adversary.

We therefore play with the set-up assumptions in order to get a stronger construction still keeping it viable in several applications, and in particular for the one that they proposed: i.e., identification through e-passports.

The set-up assumption that we consider is a trusted parameter that however does not correspond to a verifier public key, therefore we keep the PKI-less feature on the verifier side. For verifier security, by appropriately using the trusted parameters we can maintain the proof of knowledge property while at the same time the adversary can mount reset attacks. Notice that this requirement is impossible to achieve without some setup assumption, therefore this justifies the use of trusted parameters. For prover security, we show that resettable witness indistinguishability (i.e., the witness used by the prover can not be recognized by the adversary even in case it has reset capabilities) is sufficient for avoiding transferability attacks.

Concretely, our protocol is a proof of knowledge that is CR+ non-transferable with respect to *any* proof of knowledge. Our protocol therefore achieves a general non-transferability property and works in a setting that admits wide applications. The CR+ security proof of our protocol ID works as follows:

1. We use as trusted parameters, the parameters of a trapdoor commitment scheme (i.e., a commitment scheme where knowledge of a trapdoor allows one to open a commitment as any message); this will let us to prove the proof of knowledge property, as the extractor will use a secret associated to the commitment parameters, thus having an advantage with respect to the resetting adversary.
2. We add to the trusted parameters another public key $\mathtt{pk}'$; this will be used to reach a contradiction, see below.
3. We run protocol ID using as witness the secret that corresponds to $\mathtt{pk}'$ instead of the one corresponding to $\mathtt{pk}$; the resettable witness indistinguishability of ID will guarantee that the adversary will not notice any difference.
4. We assume by contradiction that the adversary transfers a proof from ID to another proof of knowledge IDR.
5. We run the extractor of IDR obtaining the secret key associated to $\mathtt{pk}$.

Even though it is possible to be more general and construct our protocol based on any Σ-protocol (these protocols are 3-round special proofs of knowledge, see [11] for the definition), we suggest an instantiation based on Schnorr's protocol [31] and argue its applicability to the e-passport framework.

4.2 Efficient Instantiation

We now describe the CR+-secure identification protocol ID.

We use the Pedersen's trapdoor commitment scheme [29], which requires a $|k|$-bit prime q, a safe prime $p = 2q+1$ and two generators g, h of the subgroup G of $Z_p^\star$ of q elements for the trusted parameters. The trapdoor is the discrete logarithm α of h with base g mod p. For language L' and an hard instance $\mathtt{pk}'$ (a randomly chosen element of G) we can simply consider G and a random element $\mathtt{pk} \in G$. A randomly chosen pair of public and secret keys can be respectively a pair $(\mathtt{pk}, \mathtt{sk})$ where $g^{\mathtt{sk}} = \mathtt{pk} \pmod p$. The public parameters are denoted by $\mathtt{crs} = (p, g, h, \mathtt{pk}')$.

The key generation procedure is used to generate the public key of a user and simply consists in picking a random element $\mathtt{sk} \in Z_q$ and setting the public key $\mathtt{pk} = g^{\mathtt{sk}} \pmod p$ and the secret key is $\mathtt{sk}$.

Let us now describe the actual interaction between a prover P that possesses a public key $\mathtt{pk}$ and the associated secret key $\mathtt{sk}$. Roughly speaking, P proves to the verifier that he knows either the discrete logarithm of $\mathtt{pk}$ (that is his secret key) or the discrete logarithm of $\mathtt{pk}'$ from the public parameters. This is done by modifying Schnorr's Σ-protocol protocol [31] in the following way. We denote the three moves of Schnorr's protocol as (A, C, Z). Here $A = g^s \pmod p$ (for a randomly chosen s in Z_q) is the first message of the prover, C is verifier's challenge (still randomly picked in Z_q) and $Z = s + C \cdot \mathtt{sk} \pmod q$ is prover's answer to the challenge C. The verifier will then check that $g^Z = A \cdot \mathtt{pk}^C \pmod p$. If the prover wants to prove knowledge of one of two discrete logarithms, he runs in parallel two instances of the protocol (one for each of the two inputs) and sends (A_0, A_1). The verifier sends one challenge C. Then the prover answers with (Z_0, C_0, Z_1, C_1) such that Z_b corresponds to Schnorr protocol's answer to (A_b, C_b) for $b = 0, 1$, and $C_0 + C_1 = C \pmod q$. This technique can be traced back to the work of [12, 11] and we will see in Fig. 2, when the prover only knows one of the two discrete logarithms, extra care must be taken to craft messages A_0 and A_1, however, as we described above, such messages do not require knowledge of the witness. In the notation used in ID, we have that $a = (A_0, A_1)$, $c = C$ and $z = (Z_0, C_0, Z_1, C_1)$. In order to obtain security against reset attacks, the verifier commits to his message using Pedersen's commitment with the parameters (g, h) from the public parameters

crs. The commitment to the challenge is sent as the first message of the identification protocol which then continues with the three-move modified Schnorr identification protocol. The resulting protocol is thus a four-move protocol. The protocol is illustrated in Figure 2.

Security Parameter: k.
Tools: pseudorandom function f.
Common input: The public information $(p, q, g, q, \mathtt{pk}')$.
P**'s identity:** $\mathtt{pk} \in G_q$.
P**'s private input:** $\mathtt{sk}$ such that $g^{\mathtt{sk}} = \mathtt{pk} \pmod p$.
P**'s randomness**: randomly pick a seed s; the randomness of P will be taken from the output of $f(s, \hat{C})$ where $\hat{C}$ is the first message received from V.

V: pick random $C \in Z_q$ and commit to C by computing $\hat{C} = g^C h^r$ for a random $r \in Z_q$. Send $\hat{C}$ to P.
P: randomly pick $s_0, C_1, Z_1 \in Z_q$, and set $A_0 = g^{s_0}$ and $A_1 = g^{z_1}\mathtt{pk}'^{-C_1} \pmod q$. A_0 and A_1 are sent to V.
V: upon receiving (A_0, A_1) open commitment $\hat{C}$ by sending (C, r).
P: check that the opening is correct and then compute Z_0 as follows: $C_0 = C - C_1 \pmod q$, $Z_0 = s_0 + C_0\mathtt{sk} \pmod q$. Send (Z_0, C_0, Z_1, C_1).
V: Accept if $C_0 + C_1 = C \pmod q$ and if $g^{Z_0} = A_0\mathtt{pk}^{C_0} \pmod p$ and $g^{Z_1} = A_1\mathtt{pk}'^{C_1} \pmod p$.

Fig. 2. Efficient CR+ Non-Transferable Identification Protocol ID_{DLOG}.

4.3 Application to E-Passports

The protocol depicted in Fig. 2 has many nice features for the e-passport system. Notice that an e-passport is equipped with an RFID chip, in particular the next generation of e-passports will make use of public-key cryptography for transferability and cloning prevention.

Another important feature is that e-passports are given to an inspector at the border control that thus has physical control of the device for a time interval. Therefore, the e-passport could in general be subject to reset attacks where the malicious inspection system will try to gain as much information as it can in order to impersonate that identity later. Moreover, it is also possible that the inspection system initiated an identification protocol with a verifier before starting his turn in the border control system and will try to continue it as soon as he will finish his turn. This setting therefore perfectly fits the CR+ notion of non-transferability. This is an important issue since in future e-passports may be used for identification in the context of various other (security) applications.

Note that in CR+ scenario the current proposal for chip authentication protocol in Extended Access Control [5] of e-passport (see 2.1 for more details) is transferable, as informally shown in Section 3.1.

The protocol that we have proposed works in the trusted parameter model. Notice that this is not an extra assumption for the application to e-passports. Indeed, e-passports are made by governments and readers at the border control already trust the parameters decided by those governments (i.e., they accept as valid the identities certified through digital signatures and digital certificates by those governments). Therefore there is no extra assumption when in the context of e-passport a government also appends to its public information the parameters that we require as trusted parameters (i.e., two group elements of G).

A further useful feature of our candidate implementation for e-passports is that there is no public-key requirement on the verifier side. Notice that, for e-passports, the management of a

PKI is problematic as it should include a key-revocation management that would be difficult to implement.

5 Conclusion

We reconsider identification protocols under the so-called reset and transferability attacks in the context of applications with enhanced and challenging security requirements. As the underlying use case we focus on electronic passports. E-passports play an important role since they concern every individual and carry sensitive personal and soon biometric information that can be subject to attacks, misuse and privacy violations. We show that the current proposal for e-passport (Extended Access Control), although using strong cryptography, it is conceptually vulnerable to those attacks, more concretely the underlying chip authentication protocol. We propose a new security definition that refines the previous definitions for resettable non-transferable identification protocols. We believe that the new notion will better capture realistic scenarios. We also propose a protocol that satisfies this definition.

The work in this paper and the new notion are informal. Currently we are working on formal definitions security proofs for the proposed protocol. We believe our work and results contribute to a more careful and sound design of applications such as e-passport that have very sophisticated security requirements to prevent misuse of citizens personal data.

Acknowledgments. The work of the authors has been supported in part by the European Commission through the FP7 Information Communication Technologies programme FRONTS (Foundations of Adaptive Networked Societies of Tiny Artefacts) under project number 215270 and in part by the European Commission through the IST program under Contract IST-2002-507932 ECRYPT.

References

1. G. Avoine, K. Kalach, and J.-J. Quisquater. Belgian biometric passport does not get a pass... your personal data are in danger! `http://www.dice.ucl.ac.be/crypto/passport/index.html`.
2. G. Avoine, K. Kalach, and J.-J. Quisquater. epassport: Securing international contacts with contactless chips. In *Proceedings of Financial Crypto 08*, 2008.
3. M. Bellare, M. Fischlin, S. Goldwasser, and S. Micali. Identification protocols secure against reset attacks. In *Advances in Cryptology - Eurocrypt 2001, Lecture Notes in Comp uter Science*, volume 2045 of *LNCS*, pages 495 – 511. Springer-Verlag, 2001.
4. S. Brands and D. Chaum. Distance-bounding protocols. In *Proceedings of Eurocrypt '93*, pages 344–359, 1993.
5. BSI. Advanced security mechanisms for machine readable travel documents – extended access control. `http://www.bsi.bund.de/fachthem/epass/EACTR03110_v110.pdf`.
6. L. Bussard and Y. Roudier. Embedding distance bounding protocols within intuitive interactions. In *Proceedings of the First International Conference on Security in Pervasive Computing (SPC'2003)*, Boppard, March 2003.
7. R. Canetti, O. Goldreich, S. Goldwasser, and S. Micali. Resettable Zero-Knowledge. In *32nd ACM Symposium on Theory of Computing (STOC '00)*, pages 235–244. ACM, 2000.
8. R. Canetti, J. Kilian, E. Petrank, and A. Rosen. Black-box concurrent zero-knowledge requires $\tilde{\omega}(\log n)$ rounds. In *33rd ACM STOC*, pages 570–579, Crete, Greece, July 6–8, 2001. ACM Press.
9. D. Carluccio, K. Lemke-Rust, C. Paar, and A.-R. Sadeghi. E-passport: The global traceability or how to feel like an ups package. In *Workshop on Information Security Applications – WISA 2006*, volume 4298 of *LncS*, pages pages 391–404. Springer, 2006.
10. D. Chaum. Designated confirmer signatures. In *Advances in Cryptology EUROCRYPT 94, Perugia, Italy*, volume 950 of *Lecture Notes in Computer Science*, pages 9–12. Springer-Verlag, 1995.

11. R. Cramer, I. Damgard, and B. Schoenmakers. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In Y. Desmedt, editor, *Advances in Cryptology – Crypto '94*, volume 839 of *Lecture Notes in Computer Science*, pages 174–187. Springer-Verlag, 1994.
12. G. Di Crescenzo, G. Persiano, and I. Visconti. Constant-Round Resettable Zero Knowledge with Concurrent Soundness in the Bare Public-Key Model. In *Advances in Cryptology – Crypto '04*, volume 3152 of *Lecture Notes in Computer Science*, pages 237–253. Springer-Verlag, 2004.
13. G.S. Kc and P.A. Karger. Security and Privacy Issues in Machine Readable Travel Documents (MRTDs). RC 23575, IBM T. J. Watson Research Labs, April 2005.
14. G. P. Hancke and M. G. Kuhn. An rfid distance bounding protocol. In *Proceedings of IEEE/Create-Net SecureComm2005*, 2005.
15. International Civil Aviation Organization. Machine Readable Travel Documents, PKI for Machine Readable Travel Documents offering ICC Read-Only Access, 2004. `http://www.icao.int/mrtd`.
16. M. Jakobsson, K. Sako, and R. Impagliazzo. Designated verifier proofs and their applications. In *Advances in Cryptology EUROCRYPT96*, Lecture Notes in Computer Science, pages 143–154. Springer-Verlag, 1996.
17. A. Juels, D. Molnar, and D. Wagner. Security and privacy issues in e-passports. In *SecureComm 2005, First International Conference on Security and Privacy for Emerging Areas in Communication Networks, Athens, Greece*, September 2005.
18. H. A. Justice. Eu standard specifications for security features and biometrics in passports and travel documents. Technical report, EU, 2006.
19. S. Kumar, C. Paar, J. Pelzl, G. Pfeiffer, A. Rupp, and M. Schimmler. How to Break DES for 8,980. In *SHARCS'06 – Special-purpose Hardware for Attacking Cryptographic Systems*, pages 17–35, 2006. `http://www.hyperelliptic.org/tanja/SHARCS/talks06/copa_sharcs.pdf`.
20. Y. Liu, T. Kasper, K. Lemke-Rust, and C. Paar. E-passport: Cracking basic access control keys with copacobana. SHARCS2007, 2007.
21. S. Micali and L. Reyzin. Min-Round Resettable Zero-Knowledge in the Public-key Model. In *Advances in Cryptology – Eurocrypt '01*, volume 2045 of *Lecture Notes in Computer Science*, pages 373–393. Springer-Verlag, 2001.
22. J. Monnerat, S. Vaudenay, and M. Vuagnoux. About machine-readable travel documents – privacy enhancement using (weakly) non-transferable data authentication. In *International Conference on RFID Security*, 2007.
23. I. T. MRTD/NTWG. Biometrics Deployment of Machine Readable Travel Documents, Technical Report, 2004. `http://www.icao.int/mrtd`.
24. I. C. A. Organization. Benefits of mrtd. `http://mrtd.icao.int/content/view/28/203/`.
25. I. C. A. Organization. Annex I, Use of Contactless Integrated Circuits In Machine Readable Travel Documents, 2004. `http://www.icao.int/mrtd`.
26. I. C. A. Organization. Machine Readable Travel Documents, Technical Report, Development of a Logical Data Structure - LDS For Optional Capacity Expansion Technologies, 2004. `http://www.icao.int/mrtd`.
27. I. C. A. Organization. Machine Readable Travel Documents, Supplement to Doc9303-part1-sixth edition, 2005. `http://www.icao.int/mrtd`.
28. I. C. A. Organization. Machine Readable Travel Documents, Doc 9303, Part 1 Machine Readable Passports, Fifth Edition, 2003.
29. T. P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In J. Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 129–140, Santa Barbara, CA, USA, Aug. 11–15, 1991. Springer-Verlag, Berlin, Germany.
30. H. Robroch. ePassport Privacy Attack, Presentation at Cards Asia Singapore, April 26,2006. `http://www.riscure.com`.
31. C. P. Schnorr. Efficient Signature Generation for Smart Cards. *Journal of Cryptology*, 4(3):239–252, 1991.
32. D. Singele and B. Preneel. Distance bounding in noisy environments. In *Security and Privacy in Ad-hoc and Sensor Networks*, pages 101–115. Springr Verlag, 2007.