A better time approximation scheme for e-passports

Charalampos Petrou, Christoforos Ntantogian, Christos Xenakis

Department of Digital Systems, University of Piraeus
Piraeus, Greece
{petrou, dadoyan, xenakis}@unipi.gr

Abstract. E-passports are the new means of identification documents in border control points, where special reader devices named inspection terminals are installed to authenticate travelers. The authentication of e-passports to inspection terminals is based on biometric data stored in the formers, while the authentication of inspection terminals to e-passports is based on digital certificates. To check the expiration date of certificates, e-passports maintain an internal variable named *effective date*, which provides only an estimation of the current time. This introduces a serious threat on e-passports' privacy. Specifically, e-passports may accept expired certificates, considering them as non-expired, due to the time difference between the effective dates of e-passports and the current time. Thus, in case an adversary obtains an expired certificate, he/she may impersonate a fake inspection terminal and compromise sensitive personal information (e.g., biometric data) from e-passports. This paper proposes a scheme that enables e-passports to update their effective dates based on the effective dates of other, more recently updated e-passports, in a secure and effective manner. In this way, more e-passports have a better estimation of the current time, reducing the time window in which an attacker can use an expired certificate. The proposed scheme minimizes the deployment complexity, since it does not require extensive modifications to the existing infrastructure, while at the same time maintains compatibility with the legacy system.

Keywords: privacy, e-passports, proxy signatures, biometric, time approximation

1 Introduction

E-passports are the new type of international identification travel documents that come to substitute the traditional passports, containing also biometric data (i.e., face, fingerprints, and iris). They are hybrid documents that combine the paper form with an embedded chip and antenna, allowing digital processing and wireless communication with special reader devices named inspection terminals (IS), installed at the border control points, as well as providing travelers' authentication. The extended access control (EAC) mechanism [1] describes the authentication procedure that takes place between an e-passport and an IS. However, because of some acknowledged security weaknesses of EAC, an enhanced version named EACv2 [2] has been released by the Bundesamt fur Sicherheit in der Informationstechnik - Germany. In EACv2, an IS and

an e-passport, first, execute the password authenticated connection establishment (PACE) protocol, which verifies that the former has authorized access to the latter. After PACE, the terminal authentication protocol is executed, which authenticates IS to the e-passport, using a challenge-response mechanism and a three-level public key infrastructure (PKI) hierarchy. On top of this hierarchy, there is the country verifier certification authority (CVCA) with a root certificate C_{CVCA}, which is also stored in all e-passports of the country. Moreover, the CVCA issues certificates for domain and foreign document verifiers (DVs), C_{DV}; while DVs issue certificates for ISs, C_{IS}. During the terminal authentication protocol, the IS conveys to the e-passport a certificate chain (C_{IS}, C_{DV}, C_{CVCA}), and the latter using its stored C_{CVCA} authenticates C_{DV} and C_{IS}. After that, the e-passport sends to IS the stored biometric data for holder's authentication. In the final step, the chip authentication procedure is performed that protects the e-passport from cloning, as well as provides a new session key for secure data transfer.

An interesting question that arises from the above hierarchy is how the certificate of an IS is canceled. A certificate revocation list cannot be applied, since e-passports cannot be online with a public directory that maintains this list. Therefore, the limited time period validity is the only way for canceling an IS's certificate. Following this, all certificates in the employed PKI hierarchy are valid for a specific time period: (i) CVCA certificates from 6 months to 3 years; (ii) DV certificates from 2 weeks to 3 months; and (iii) IS certificates from 1 day to 1 month [3]. The lifetime of e-passports also vary from 5 to 10 years. Before the expiration of a certificate, the responsible entity requests for a new one from the upper layer of the hierarchy (i.e., an IS from a DV, and a DV from a CVCA). However, a CVCA, which resides at the top layer of the hierarchy, updates its certificate by itself using forward certificate chains [2].

Nevertheless, checking the expiration date of an IS's certificate cannot be effectively performed, since e-passports are passive RFID devices that cannot maintain an internal clock. For this reason, e-passports sustain an internal variable named *effective date*, which provides an estimation of the current time for checking certificates' expiration date. Initially, the effective date is set up equal to the time the e-passport is created, and as the e-passport passes through ISs, its effective date is updated with the most recent time value of the certificates that it receives from ISs in the certificates' chains (C_{IS}, C_{DV}, C_{CVCA}). However, this scheme provides only an approximation of the current time, introducing a serious threat on e-passports' privacy [4-11]. More specifically, e-passports may accept expired certificates, considering them as non-expired, due to the time difference between the effective dates of the e-passports and the current time. Thus, in case that an adversary obtains an expired certificate, he/she can exploit it to impersonate a fake IS and compromise sensitive personal information (e.g., biometric data) from e-passports.

This paper proposes a scheme that enables e-passports to update their effective dates based on the effective dates of other, more recently updated e-passports, in a secure and effective manner. In this way, more e-passports have a better estimation of the current time, reducing the time window in which an attacker can use an expired certificate to impersonate a fake terminal. To achieve this, the interacting e-passports and ISs exchange and store the most recent effective dates that they possess using the

following rules: (i) if the e-passport has a newer effective date compared to this the IS, then the latter updates its effective date with the effective date of the former, or (ii) if the e-passport has an older effective date than the IS's one, then the e-passport updates its effective date with the effective date of the IS. The security of the proposed scheme is based on proxy signatures [12]. In particular, the e-passports and ISs verify proxy signatures, created on behalf of a trusted CVCA, before updating their effective dates. The proposed scheme minimizes the deployment complexity, since it does not require extensive modifications to the existing infrastructure, while at the same time maintains compatibility with the legacy system.

The rest of the paper is organized as follows. In section 2 the related work is presented. Section 3 elaborates on the proposed scheme by analyzing its key components and functionality. Section 4 evaluates our proposal and finally, section 5 concludes the article.

2 Related Work

Recently, a few solutions to protect e-passports from the fake terminal attack have been proposed. In [7], the use of trusted time servers has been proposed to update e-passports' current time, using digitally signed timestamps. However, the servers' source of time is not defined, enabling the occurrence of a far-in-the-future denial of service attack. That is, the time of an e-passport is updated with an effective date far in the future. As a result, the e-passport will deny all the received certificates, because it considers them expired. In [6], the enhancement of e-passports with displays and buttons has been proposed. Based on these, the critical decision for an expired date will be taken by the e-passport's holder, who stops or allows the procedure using the button. However, semi-automated procedures may lead to users' dissatisfaction, making this solution inacceptable. Moreover, in some cases the owners give their e-passports to professionals for authentication purposes, e.g., hotel reception, bank cashier, etc., where they do not have the full control of them.

In [8], a new protocol, called on-line secure e-passport protocol (OSEP) is introduced. OSEP provides an active monitoring system, at the level of IS, that attempts to detect criminal behaviors. Additionally, OSEP includes a mutual authentication protocol between e-passports and ISs, enhancing the security of EAC. A variation of OSEP is proposed in [9] that uses elliptic curves, instead of Diffie-Hellman key agreement. An important weakness of OSEP (using either Diffie-Hellman key agreement or elliptic key cryptography) has to do with the prerequisite of online connectivity between ISs and DVs, which cannot be implemented, for example, in cases of cross-border trains and ships.

In [10], an identity based cryptography scheme is proposed, where the public keys are the users' identities. It avoids the complexity of a PKI deployment and maintenance, but it requires extensive modifications to the legacy system. Finally, in [11], a key management infrastructure is proposed, which allows dynamic update of the access keys used in EACv1. It requires less time and memory, compared to the legacy system; and the authors have implemented a prototype of this, using open-

source tools. However, many important issues have not been analyzed yet, such as the required complexity for keys' synchronization among servers. Moreover, there is no recovery process, which means that if a list of keys is compromised, all e-passports should be recalled.

A common limitation of the aforementioned solutions is that their deployment requires extensive modifications to the existing infrastructure. In particular, they propose the replacement of EAC with new protocols, which are not compatible with the existing PKI infrastructure. Moreover, they apply cryptographic functions (e.g., identity based cryptography), which have not been applied in real environments, and, therefore, their practical acceptance is limited.

3 Proposed Scheme

The proposed scheme enables e-passports to update their effective dates based on the effective dates of other, more recently updated e-passports, in a secure and effective manner. A key characteristic of this scheme is that its deployment does not require extensive modifications to the existing infrastructure, while at the same time maintains compatibility with the legacy system. To achieve this objective, it does not introduce any new protocol or entity, but rather extends the functionality of the existing ones in the legacy system. Thus, as in the legacy system, the proposed scheme consists of: (i) the e-passports, (ii) the inspection-update terminals (ISU) that interacts with the e-passports, (iii) the CVCAs, and (iv) the update and extended access control (UEAC) procedure. For the security of the exchanged effective dates, the proposed scheme applies proxy signatures, where e-passports sign their effective dates on behalf of trusted CVCAs. The aforementioned components are enhancements of their counterparts in the legacy system. In particular, the e-passports are enhanced to store the proxy key and the related certificate (see sect. 3.2). The ISU is an extension of the IS, maintaining also the most recent effective date received from e-passports. The CVCAs are enhanced to store and provide a backward certificate chain. Finally, the UEAC procedure, which is an extension of the legacy EACv2 procedure, is used for the mutual authentication between the e-passports and ISUs, as well as also for updating their effective dates.

3.1 Proxy signatures

An e-passport updates its effective date by interacting with an ISU that stores updated effective dates of other e-passports. A question that arises is how the e-passport can verify the validity of the effective date that receives from the ISU. A possible solution would be the CVCA entity to sign the effective dates, before they are stored in the ISU. In this way, the e-passport or the ISU could verify the signature of an effective date using the public key of the CVCA. Although this solution seems to be effective and secure, it cannot be directly applied, because the CVCAs do not participate in the communication between the e-passports and ISUs.

To overcome this limitation, the proposed scheme applies proxy signatures [12] and specifically the proxy-unprotected mono-signature scheme [13], which is based on the RSA-based key pair. This scheme allows maximum compatibility with the legacy system, which also uses the RSA algorithm. Generally speaking, the main objective of proxy signatures is to delegate a *proxy signer* to sign on behalf of the *original signer*. To achieve this, the original signer using his/her private key and a random value, creates a proxy key, which is securely delivered to the proxy signer. The latter can sign messages, on behalf of the original signer, using a proxy signing algorithm and the proxy key. On the other hand, for verifying proxy signatures, only the original signer's public key is required.

In the proposed scheme, the original signer is a CVCA that generates proxy keys using its private key. On the other hand, the proxy signer is an e-passport that uses a proxy key to generate and verify the proxy signatures of the effective dates. More specifically, assume that the CVCA's certificate includes the public key *e*, while the corresponding private key is *d*. This public-private RSA key pair (*e*, *d*) satisfy $ed = 1 mod \varphi(n)$, where $\varphi(n)$ is the Euler-Totient function and $n = pq$ where p, q are large primes randomly selected. The CVCA generates a proxy key *u* as follows:

$$u = h(CVCA\_id, SN)^{-d} \bmod n \quad (1),$$

where CVCA_id is an identifier of the CVCA, SN is a sequence number and h() denotes a hash function. The CVCA_id, SN and the public modulus *n* are all included in the CVCA certificate, which also contains the public key *e*. This CVCA certificate is defined as *signer CVCA certificate* and is denoted as C_{signer}.

3.2 E-passports

An e-passport stores the most recent certificate received from the interacting ISUs and, additionally, the proxy key *u*, as well as the signer CVCA certificate C_{signer}. The proxy key *u* and the C_{signer} do not change for the lifetime of the e-passport and are stored in a tamperproof and read-only memory area of it. For the creation of a proxy signature on an effective date (denoted as Eff.Date), the e-passport first selects an integer $t \in [1, n]$. Next, using the public key e, which is retrieved from the signer CVCA certificate C_{signer}, it produces the value *r* as follows:

$$r = t^e \bmod n \quad (2).$$

Next, it generates the values *k* and *y* as follows:

$$k = h(Eff.Date, r) \quad (3),$$

$$y = t\, u^k \bmod n \quad (4).$$

The pair (*k*, *y*) constitutes the proxy signature.

In order to verify a proxy signature, an e-passport, first, computes *r´* as follows:

$$r' = y^e\, h(CVCA\_id, SN)^k \bmod n \quad (5),$$

and, then, it verifies that:

$$h(Eff.Date, r') = k \quad (6).$$

This verification holds because:

$$r' = y^e\, h(CVCA\_id, SN)^k$$

$$= t^e\, u^{k\,e}\, h(CVCA\_id, SN)^k$$

$$= t^e\, h(CVCA\_id, SN)^{-k}\, h(CVCA\_id, SN)^k$$

$$= t^e = r \bmod n \quad (7).$$

3.3 CVCA

A CVCA generates and maintains both a forward and backward certificate chains. When the CVCA generates a new public-private key pair, it issues two different certificates: one for the forward CVCA certificate chain and another for the backward CVCA certificate chain. More specifically, assume that the CVCA has the public-private key pair (e_i, d_i) and generates a new key pair (e_{i+1}, d_{i+1}). In this case, two certificates are created. The first certificate is created for the forward CVCA certificate chain and includes the public key e_{i+1} signed by the old private key d_i. The second certificate (i.e., backward CVCA certificate chain) includes the old public key e_i signed by the new private key d_{i+1}.

To better understand the above notions, we use the following example: Assume that a CVCA has generated four public - private key pairs (see Fig. 1). That is, (e_1,d_1), (e_2,d_2), (e_3,d_3), (e_4,d_4), where (e_1,d_1) is the first generated pair and the (e_4,d_4) the last. In this case, the certificates C_1, C_2, C_3 constitute the forward CVCA certificate chain. For example, the certificate C_2, which includes the public key e_3 (with corresponding private key d_3), has been signed by the private key d_2. On the other hand, the certificates C_4, C_5, C_6 constitute the backward CVCA the certificate chain. For example, certificate C_5, which includes the public key e_2 (with corresponding private key d_2), has been signed by the private key d_3.

As mentioned previously, the CVCA generates the proxy keys that are used from e-passports to create the proxy signatures of their effective dates. A proxy key is generated using the private key of the CVCA certificate (see eq. 1). Note that the CVCA certificate can be either a forward or a backward CVCA certificate. In this paper, we arbitrary choose that all proxy keys are generated by forward CVCA certificates.

3.4 ISU

ISUs are installed at the border control points and inspect the passing e-passports using the UEAC procedure. Apart from the inspection functionality, the ISUs update also the effective dates of the e-passports. To support this additional functionality, the ISUs store for each country: (i) the most updated effective date, (ii) the corresponding proxy signature of the effective date, (iii) the related signer CVCA certificate, (iv) the

forward CVCA certificate chain, and (v) the backward CVCA certificate chain. The signer CVCA certificate stored in an ISU will be denoted as $C_{ISU\text{-}signer}$. Note that whenever a new public-private key is generated from a CVCA, the latter delivers to the ISUs both the forward and backward CVCA certificates to update accordingly their CVCA certificate chains.

3.5 UEAC

Similarly to EACv2, the UEAC includes the PACE, terminal authentication and chip authentication protocols. The extra functionality of UEAC is the update procedure, which is executed after the successful completion of the chip authentication. The aim of this procedure is to effectively and securely update the effective dates between ISUs and e-passports. All messages exchanged for this purpose are protected by the session keys derived from the chip authentication.

Since the PACE, terminal authentication and chip authentication protocols are performed as in the legacy EACv2, we do not analyze them. In the proposed update procedure, the involved ISU, first, delivers to the e-passport an *Update Info message* that includes the following: (i) the proxy signature, (ii) the related effective date; (iii) the forward CVCA certificate chain; (iv) the backward CVCA certificate chain; and (v) the signer CVCA certificate $C_{ISU\text{-}signer}$ that is required for the verification of the proxy signature. Upon receiving this message, the e-passport checks the validity of the received proxy signature, by verifying the received signer certificate $C_{ISU\text{-}signer}$. We identify two possible scenarios for verification of $C_{ISU\text{-}signer}$: a) the signer CVCA certificate $C_{ISU\text{-}signer}$ is older than the signer CVCA certificate C_{signer} of the e-passport, and b) the signer CVCA certificate $C_{ISU\text{-}signer}$ is newer than the signer CVCA certificate C_{signer} of the e-passport.

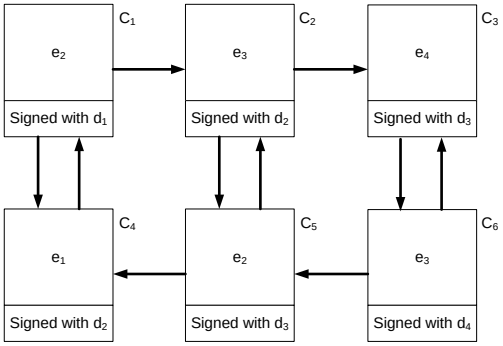

Fig. 1. Forward and backward CVCA certificate chains

In the first case, the e-passport should use the forward CVCA certificate chain for the verification of $C_{ISU\text{-}signer}$. That is, starting from its signer CVCA certificate C_{signer}, it uses the public keys of old certificates to verify the next certificates, until it reaches and verifies the signer CVCA certificate $C_{ISU\text{-}signer}$. For example (see Fig. 1), assume that the certificate C_3 is the signer CVCA certificate $C_{ISU\text{-}signer}$ and the certificate C_1 is

the signer CVCA certificate C_{signer} of the e-passport. In this case, the e-passport first verifies the certificate C_2 using C_1 and, subsequently, verifies C_3 (i.e., the signer CVCA certificate $C_{ISU\text{-}signer}$) using C_2. In the second scenario, the e-passport uses the backward CVCA certificate chain to verify the signer CVCA certificate $C_{ISU\text{-}signer}$. For example (see Fig. 1), assume again that the certificate C_2 is the signer CVCA certificate C_{signer} and the certificate C_1 is the signer CVCA certificate $C_{ISU\text{-}signer}$. The e-passport first verifies the certificate C_5 using C_2 and then, it verifies C_4 using C_5. Finally, the e-passport verifies C_1 (i.e., the signer CVCA certificate $C_{ISU\text{-}signer}$) using C_4.

After the successful verification of the signer certificate $C_{ISU\text{-}signer}$, the e-passport extracts from it the necessary values *e*, *n*, *SN*, *CVCA_id* (see sect. 3.1). If the proxy signature is valid, then the e-passport compares the received effective date with its own one. If the effective date of the ISU's certificate is more recent, then the e-passport updates its own effective date. In this case, the e-passport simply sends to ISU an *Update End* message with empty content, finalizing the procedure. On the other hand, if the effective date of the e-passport is more recent, then the e-passport signs its effective date using its stored proxy key. Next, the e-passport sends to the ISU an *Update End* message that includes the effective date, the related proxy signature and the signer certificate C_{signer}. Upon receiving the *Update End* message, the ISU obtains the appropriate values from the signer certificate C_{signer} and proceeds with the verification of the proxy signature (see eq. (6) and (7)). If it is successful, the terminal checks that the effective date is indeed more recent from its stored one. If yes, the ISU updates its effective date and stores the proxy signature, as well as the e-passport's signer certificate (i.e., $C_{ISU\text{-}signer} = C_{signer}$).

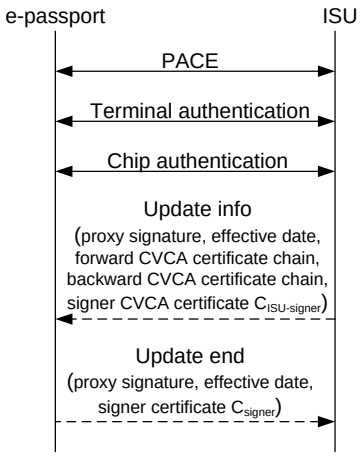

Fig. 2. UEAC execution

4 Evaluation

The proposed scheme mitigates the threat of compromised expired certificates, since an adversary can use them for a more limited time period to impersonate a fake termi-

nal. This happens because the proposed scheme allows e-passports to update their effective date based on the effective date of other e-passports. In this way, more e-passports have a better time approximation compared to the legacy system. This can be justified as follows. Assume the owner of an e-passport with an updated effective date plans to travel. During traveling, the e-passport interacts with ISUs, which update their effective dates with the effective date of the updated e-passport. The ISUs in turn will update the effective dates of other e-passports (i.e., not updated) that interact with. In other words, the updated effective date of one e-passport propagates to other e-passports through ISUs. On the other hand, in the legacy system the e-passports update their effective dates using only the effective dates found in the certificate chains (C_{IS}, C_{DV}, C_{CVCA}).

One can argue that in case an ISU has not interacted with any e-passport for a long time, then it may be possible that its effective dates are not updated. However, assuming that in each country there is a critical mass of frequent travelers, the majority of ISUs in a country will have updated effective dates. The approximation of the effective dates of the e-passports with the current time depends on the time that the e-passports will interact with the ISUs. That is, if an ISU has just received a newly issued certificate and an e-passport happens to interact with the specific ISU, then the effective date of this e-passport will have a very good approximation to the current time. Note that the validity period of PKI certificates depends on the configuration of each national PKI [3].

The possibility of a fake terminal attack is also mitigated by the fact that an adversary, in order to perform this attack, should not only compromise an ISU certificate, but also possess a valid proxy signature. However, proxy signatures can be produced only by an authentic e-passport or a CVCA, as these two entities are the only authorized proxy key owners. However, it is considered that these keys in CVCAs are securely generated and stored, while in e-passports they are stored in a tamperproof read/write protected area. Moreover, a proxy key is never conveyed during the UEAC execution, eliminating the possibility an attacker to eavesdrop and obtain it. Even if an adversary obtains a valid certificate of an ISU, it cannot force an e-passport to sign a chosen effective date, since the proxy signature is produced only after the e-passport verifies that the ISU possesses also a valid signature.

One of the key advantages of the proposed scheme is that its deployment does not require extensive modifications to the existing infrastructure. The functionality of the e-passports, ISU and the UEAC protocol are extensions of the e-passports, IS and EAC, respectively, of the legacy system. The CVCAs are additionally required to store and maintain the backward CVCA certificate chain for the verification of the proxy keys. Moreover, the proposed scheme uses the same PKI hierarchy of the legacy system.

Finally, the communication overhead caused by the execution of the update procedure in UEAC is negligible, since it includes only one message exchange round (see Fig. 2). On the other hand, the computational overhead of the proposed scheme depends on the number of certificates in the forward and backward CVCA certificate chains that an e-passport should examine to reach and verify a signer CVCA certificate. In the base case scenario, the e-passport should verify only one (1) certificate in

the forward certificate chain to reach the signer CVCA certificate. On the other hand, the worst case scenario happens when the e-passport has been issued long time ago, and the validity period of the CVCA certificates is the minimum one, which is six months. In this case, assuming that the e-passport has a lifetime of 10 years and the $C_{ISU\text{-}signer}$ is the most recently issued CVCA certificate, the e-passport should verify14 different forward CVCA certificate chains to reach the signer CVCA certificate.

5 Conclusions

This paper proposes a scheme that enables e-passports to update their effective dates based on the effective dates of other, more recently updated e-passports, in a secure and effective manner. In this way, the e-passports have a better estimation of the current time, reducing the time window in which an attacker can use an expired certificate to impersonate a fake terminal. In the proposed scheme, an ISU and an e-passport execute the UEAC procedure to update their effective dates. To verify the authenticity of the effective dates and protect against malicious actions, the ISU and the e-passport verify proxy signatures, created on behalf of a trusted CVCA. Finally, the proposed scheme minimizes the deployment complexity, since it does not require extensive modifications to the existing infrastructure, while at the same time maintains compatibility with the legacy system.

6 References

1. Bundesamt fur Sicherheit in der Informationstechnik (BSI), Germany: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), version 1.0, TR-03110, 2006
2. Bundesamt fur Sicherheit in der Informationstechnik (BSI), Germany: Advanced Security Mechanisms for Machine Readable Travel Documents - EAC, PACE and RI, version 2.0 TR-03110, 2008
3. Commission Decision C (2006) 2909, EU – E-passport Specification, 28.06.2006
4. Rishab Nithyanand, "A Survey on the Evolution of Cryptographic Protocols in e-passports" University of California – Irvine 2009
5. Anshuman Sinhahttp://www.sciencedirect.com/science/article/pii/S187454821100045X - af000005, "A survey of system security in contactless electronic e-passports", International Journal of Critical Infrastructure Protection Volume 4, Issues 3-4, December 2011, Pages 154-164
6. Rishab Nithyanand, Gene Tsudik, and Ersin Uzun, "Readers Behaving Badly Reader Revocation in PKI-Based RFID Systems", Computer Security – ESORICS 2010 Lecture Notes in Computer Science, 2010, Volume 6345/2010, 19-36
7. Markus Ullmann and Matthias Vögeler, "Contactless Security Token Enhanced Security by Using New Hardware Features in Cryptographic-Based Security Mechanisms" from "Towards Hardware-Intrinsic Security Information" Security and Cryptography, 2010, Part 5, 259-279, chapter 4.4

8. Vijayakrishnan Pasupathinathan, “An on-line secure e-passport protocol”, ISPEC'08 Proceedings of the 4th international conference on Information security practice and experience, Pages 14-28
9. Abid, M., Afifi, H.: Secure e-passport protocol using elliptic curve diffie-hellman key agreement protocol. In: 4th International Conference on Information Assurance and Security. (2008)
10. C.H. Li, X.F. Zhang, H. Jin, W. Xiang, “E-passport EAC scheme based on Identity-Based Cryptography”, Information Processing Letters 111 (2010) 26–30
11. Pablo Najera, Francisco Moyano, Javier Lopez, “Security Mechanisms and Access Control Infrastructure for e-passports and General Purpose e-Documents”, Journal of Universal Computer Science, vol. 15, no. 5 (2009), 970-991
12. Mambo, Masahiro, Keisuke Usuda, and Eiji Okamoto, "Proxy signatures for delegating signing operation", Proceedings of the 3rd ACM conference on Computer and communications security, ACM, 1996.
13. Z. Shao, “Proxy signature schemes based on factoring”, Information Processing Letters, Vol. 85, pp. 137–143, 2003.