Journal of Computer Security 22 (2014) 1025–1049
DOI 10.3233/JCS-140522
IOS Press

Towards a more secure and scalable verifying PKI of eMRTD

Nicolas Buchmann [*] and Harald Baier

da/sec Biometrics and Internet Security Research Group, Hochschule Darmstadt, Darmstadt, Germany
E-mails: {Nicolas.Buchmann, Harald.Baier}@h-da.de

The new electronic passport stores biometric data on a contactless readable chip to uniquely link the travel document to its holder. This sensitive data is protected by a complex protocol called Extended Access Control (EAC) against unlawful readouts. EAC is manifold and thus needs a complex public key infrastructure (PKI). Additionally EAC is known to suffer from unsolved weaknesses, e.g., stolen (mobile) passport inspection systems due to its missing revocation mechanism. The article at hand seeks for potential approaches to solve these shortcomings. As a result we present an evaluation framework with special focus on security and scalability to assess the different candidates and to give a best recommendation. Instead of creating new protocols, we focus on solutions, which are based on well-known protocols from the Internet domain like the Network Time Protocol (NTP), the Online Certificate Status Protocol (OCSP), and the Server-based Certificate Validation Protocol (SCVP). These protocols are openly standardised, thoroughly tested, interoperable, and with the exception of SCVP all widely deployed. In addition to these Internet protocols we evaluate state-of-the-art security protocols proposed by the scientific community, e.g., the Hoepman protocol, the BioPACE V2 protocol and the On-line Secure E-Passport Protocol (OSEP). Our recommendation is that the EU EAC PKI would benefit most from introducing NTP and OCSP, or if fine-grained access control of EAC are considered dispensable by introducing the BioPACE V2 protocol.

Keywords: eMRTD, revocation, security, Extended Access Control

1. Introduction

Travel documents have become a natural part of travelling into foreign countries for citizens. The best known and most frequently used travel document is the passport. According to [14] the passport is the basic official document, which denotes a person's identity and citizenship and provides an assurance for the state of transit or destination that the holder can return to the state of issuance. For international operability passports are specified by the International Civil Aviation Organisation (ICAO), who sets the standards for all its contracting states.

[*] Corresponding author: Nicolas Buchmann, da/sec Biometrics and Internet Security Research Group, Hochschule Darmstadt, Mornewegstraße 32, 64293 Darmstadt, Germany. Tel.: +49 6151 16 75071; Fax: +49 6151 16 4825; E-mail: Nicolas.Buchmann@h-da.de.

1.1. Context

The ePassport is a new passport with capabilities for biometric identification with the help of a contactless integrated circuit chip. It is intended to achieve a new level of travel document security, by a strong bond between the electronic Machine Readable Travel Document (eMRTD) and its holder [14]. Passengers will, besides the security advantages, profit from faster border control clearance times, because of the possible automation of the border control. However the storage of biometric data and the wireless interface of the chip lead to security concerns, e.g., the leakage of personal data. The European Union (EU) addresses these worries by implementing an additional security protocol called *Extended Access Control* (EAC) [6], which aims at protecting the citizen's sensitive data by only granting access to authorised parties as defined by the issuing country.

1.2. Motivation

EU EAC is on the one hand very powerful and can satisfy nearly all security and privacy demands. On the other hand, however, it requires a very complex public key infrastructure (PKI) to ensure the authenticity and authorisation of inspection systems [13,15]. We call this public key infrastructure the *Verifying PKI*. As of today the Verifying PKI does not have a mechanism for revocation. To limit the value of a stolen inspection system the issued inspection system certificates have a very short validity period, usually only one day. This creates an enormous effort with respect to both generation of key pairs/certificates and their distribution, because currently every inspection system needs a new certificate everyday, for each country that issues an EAC enabled eMRTD.

In addition to the complexity of the key generation and certificate distribution, an attacker may abuse a stolen inspection system for two main reasons: first, the certificate is valid for its entire validity period and cannot be revoked. Second the eMRTD does not have an accurate time source. Thus in general the eMRTD is not able to detect an expired certificate, which extends the possible attack period. Introducing a reliable revocation system would not only make EAC more secure, but also would lower the burden for creating certificates with extremely short validity periods.

The complexity of the Verifying PKI and the obvious inadequacies of the EU EAC protocol are the starting point of the article at hand. Finding and evaluating possible solutions for the shortcomings of EAC are the main goals of this article. Although EAC and its Verifying PKI is used within the European Union, there is no discussion about the aforementioned drawbacks in the standardisation documents. Although the scientific community identified some weaknesses and came up with solution candidates (e.g., [9,13,26,28]) there is no evaluation of the candidates and thus no best recommendation. Additionally if a solution is given, it is usually self-created instead of using well-established standards.

1.3. Results and contributions

This article builds on preliminary results from [3], which we refine with new findings from the scientific community [4,8,25] and assess these with the evaluation scheme presented in [3]. Our first contribution is to extend the discussion of [3,13,26] and to highlight the two main shortcomings of the EU EAC, namely the missing revocation mechanism of inspection systems and the absence of an accurate time source of an eMRTD. We then discuss the resulting potential risks. In order to strengthen EAC we present solution candidates. In addition to previously proposed enhancements of the community (e.g., [13]), we introduce two promising approaches: first, as an authentic and precise time source the Network Time Protocol (NTP, [21]) is proposed together with the Online Certificate Status Protocol (OCSP, [16]) as lightweight revocation mechanism. Second the Server-based Certificate Validation Protocol (SCVP, [19]) is assessed, which transfers the certificate chain validation, the time acquirement, and the revocation check to an external server. In contrast to existing proposals using these proven Internet standards is also a design choice with the future in mind, because the next generation of smart card technology will be able to directly communicate via TCP/IP [24,29]. As with all new technologies this feature will at first be solely available in high-end smart cards. In compliance with Moore's law TCP/IP will in the near future become available in cheap mass-produced bulk smart cards. This can be justified simply because TCP/IP is widely adopted in a variety of other domains and will provide a huge gain of comfort and interoperability. eMRTDs today are based on smart card technology and future generations of eMRTDs can benefit from technical advances in smart card technology. An envisioned future eMRTD supporting IP will most likely not communicate to the Internet directly, but with assistance of the terminal as proxy to handle network subtleties like DNS or routing.

In order to come up with our best recommendation for an actual practical use, we develop an assessment methodology with a special focus on security, scalability, and standardisation. We evaluate the candidates against our weighted criteria. We also evaluate our proposal against the two currently most promising approaches from the scientific community, the Hoepman protocol [13], and the BioPACE V2 protocol [4]. The final outcome is that the Verifying PKI would benefit most from introducing NTP and OCSP, or if fine-grained access control of EAC are considered dispensable by introducing BioPACE V2. Assuming an online connection of the inspection system with a sufficient bandwidth is reasonable even in the scope of mobile terminals due to the pervasiveness of UMTS/LTE.

1.4. Organisation of this article

The rest of the article is organised as follows: Section 2 summarises related contributions, places our work in the context of these papers, and demonstrates the gap in existing research, which is filled by our work. After presenting the related work, Section 3 describes the status quo of the security infrastructure of eMRTDs. Then Section 4 explains the shortcomings of the current security protocols and presents potential solutions of these weaknesses. We develop our weighted assessment methodology in Section 5, evaluate the Internet domain solution candidates, the Hoepman protocol and the BioPACE V2 protocol against our list of criteria. Finally, Section 6 concludes our article and points to future work.

2. Related work

This section summarises related contributions, places our work in the context of these papers, and demonstrates the gap in existing research, which is filled by our work.

Moses [26] gives in his white paper from Entrust a comprehensive view on the weaknesses of the current Verifying PKI and proposes a workaround. Instead of revoking the certificates and providing a real-time clock, he proposes to compensate this deficiency with strong confidential storage and restriction of using the reader's private key to authorised operators, e.g., due to a storage of the private key in the back office. His self-assessment of this solution is 'brittle, because there is no way to recover when it goes wrong'. In contrast our solution also works if the terminal's private key has already been compromised. Moses [26] states that the absence of a real-time clock makes revocation ineffective. We agree with this statement and will only evaluate solutions that provide a real-time clock and revocation.

Hoepman et al. [13] present weaknesses and propose security improvements for a variety of eMRTD protocols. Relevant for our article are only the proposed improvements for EAC. Hoepman et al. [13] sketch an idea of a self-invented online terminal authentication (Hoepman protocol) and define certain boundary conditions (e.g., resistance to replay attacks). The proposed protocol is actually very similar, to one of our proposals, the SCVP protocol (see Section 4.2.3). It also delegates the actual terminal authentication to a trusted third-party called Application Authority (*AA*). However, in contrast to our SCVP proposal the Hoepman protocol separates the terminal access rights from the terminal certificates. Hoepman et al. [13] refer to the terminal certificate as C_{AA} which contains the public key K_{TA} and is signed by the *AA*. They describe there proposed protocol as such:

> First, the terminal sends the certificate C_{AA} (containing its public key K_{TA}) to the chip. The chip and the terminal perform a challenge-response protocol in which the terminal proves to the chip that it owns the private key corresponding to K_{TA}. This establishes the identity of the terminal. Next, the chip sets up an authenticated channel between itself and the back office of the issuing country. It can do so using a country certificate that is stored in the chip during personalisation. The channel should not be vulnerable to replay attacks. It sends C_{AA} (and K_{TA}) to the back-office. There, C_{AA} is verified against the known application authorities (this

validates that K_{TA} was certified by such an authority) and K_{TA} is checked against the list of all revoked terminals. If these checks pass, the access rights for *AA* are sent back to the chip. If not, then the empty set (i.e., no access rights) is sent back to the chip. The chip interprets the access rights it receives and grants access to the terminal accordingly. Because the channel is authentic and does not allow replay attacks, the access rights received by the chip correspond to the certificate it sent to the back office.

Although this is a promising approach, which provides real-time revocation, it suffers from two drawbacks: first, there is no detailed specification of the mechanism. Second it is a new protocol, which has to be investigated thoroughly. Our solution candidates, however, are mostly based on well-known and well-established Internet standard protocols that have been proven useful in other domains for a long time. Additionally Hoepman et al. [13] do not provide an assessment methodology to evaluate solution candidates. Nevertheless we will evaluate the Hoepman online terminal authentication, because in our opinion it is currently one of the most promising, self-created approaches from the scientific community.

Vaudenay and Vuagnoux [33] report the weaknesses of EAC and describe certain attack scenarios, but do not propose improvements for EAC.

Chaabouni and Vaudenay [9] introduce the idea to have identity checks when leaving a domestic country to have more frequent clock updates. To provide certificate revocation they propose a reputation-based trust mechanism where a threshold authentication proof is created by a collaboration of a certain number of neighbour terminals. The proposed additional identity check does indeed shorten the possible attack period, but it does not completely solve the problem, because during a long vacation an eMRTD's date is still not up-to-date. A reputation-based revocation system solves the problem of a single stolen terminal, but the authors present no detailed analysis how to integrate such a revocation system in the eMRTD infrastructure. An attacker still has the option to steal a sufficient number of terminals and compromise them to exceed the threshold for the authentication proof. We propose solutions that provide a real-time date and revocation independent of the number of stolen terminals by an attacker.

Chaabouni extends his ideas from [9] in [8] by presenting an actual implementation for a t-out-of-l threshold signature scheme to augment terminal authentication. His scheme is based on RSA threshold signatures and the actual revocation check is performed by the neighbouring terminals. The main motivation for this approach given by the paper is the fact that terminals have a real clock embedded and more computational power than eMRTDs and are therefore better suited for checking the revocation status. Even though this is true and the steps from the theoretic idea [9] to an actual implementation [8] should be sincerely acknowledged the basic idea still suffers from the same problems as discussed for [9], and now with an actual implementation surface some new deficiencies. An attacker can still steal t-out-of-l terminals to exceed the threshold, which is a relevant problem simply because why should an attacker perform the illegal act of breaking and entering to only steal one terminal and not t terminals. Another problem with the threshold mechanism is that it does not consider small border check stations (or less affluent countries) with only two to three mobile terminals which make a threshold system nearly pointless. In our opinion the biggest problem with the proposed scheme is that it relies on the assumption that Document Verifiers are trusted participants. This might be true for the majority of DVs, but should not be a general rule, because such a revocation mechanism is powerless against rogue DV certificates and trust issues towards DVs in countries with poor relations. A revocation mechanism in the eMRTD domain is only needed in rare special cases, but if it is needed it should be powerful enough to cover all use cases, which the proposed scheme does not fulfil.

Li et al. [25] present an EAC scheme using identity-based cryptography (IBC) and compare it to the EU EAC system as well as the Singapore EAC scheme [31]. This new authorisation mechanism based on IBC introduces an authentication protocol between the eMRTD chip and a new entity the so called authorised smartcard. Every terminal needs such an authorised smartcard which stores its public identity information, and in the secure internal memory the terminal's private key. Instead of relying on the Verifying PKI the scheme needs an IBC server system for every eMRTD issuing country to provide the cryptographic services, and the authorisation information are now stored inside the authorised smartcard instead of the terminal certificates. The attack scenario therefore shifts from stealing a terminal to stealing an authorised smartcard. Therefore the authors introduce the concept of smartcard revocation lists which are stored in data group 13 of the eMRTD. Updating this revocation list is only allowed by a domestic terminal after a successful check. Even so the authors claim that their scheme is less complex than the EU EAC SPOC infrastructure their system relies on an on-line IBC server system to refresh the IBC information after expiration on the authorised smartcard. It puzzles us that this new EAC scheme relies on an on-line system, but the revocation system is constructed from a primitive off-line revocation list system. Since the updates of the revocation lists are only performed if the eMRTD is successfully checked by a domestic terminal, the document holder is not protected against stolen terminals during a stay abroad or a travel between two foreign airports. At a first glance the proposed IBC EAC system might seem cheaper to maintain, than EU EAC because no more Verifying PKI is needed, but on the one hand the IBC servers have to be constantly on-line too, and on the other hand every terminal now needs an authorised smartcard. Together with the proposed primitive off-line revocation mechanism we identify as biggest difference to the current EU EAC system, that the authors replace the current EU terminal authentication, which relies on the security of RSA signatures or ECDSA signatures, with an authentication protocol that relies on the security of the ECDLP and the bilinear Diffie–Hellman problem. This might be interesting from a cryptographic perspective, but does not solve the problem of stolen terminals.

Deufel et al. [11] propose to replace the knowledge based secret (e.g. the Machine Readable Zone (MRZ)) of the Password Authenticated Connection Establishment

(PACE) protocol by a biometric-based secret instead. The protocol in its initial form is called BioPACE and extended by Buchmann et al. [4] in the form of BioPACE Version 2 (BioPACE V2). Since BioPACE V2 fixes a tracking issue, and creates a link between the physical document and the chip we will focus our discussion on BioPACE V2. The authors discuss the expediency of replacing EU EAC with BioPACE V2. BioPACE V2 is a preprocessing step, which is based on the ISO/IEC 24745 standard [23] for biometric information protection, for the PACE protocol. During personalisation of an eMRTD the biometric modality is enrolled and a feature extraction from the captured biometric sample results in a biometric reference comprising of a pseudonymous identifier *PI* and auxiliary data *AD*.

After the personalisation BioPACE V2 is ready for the actual verification which is depicted in Fig. 1. A verification consists of a new feature extraction from a fresh biometric sample and the previous enrolled *AD*. The verification results in a new pseudonymous identifier *PI**, which equals *PI* if and only if the same person provided the biometric sample and therefore a biometric match occurs. BioPACE V2 is a preprocessing step for PACE, because after calculating *PI** it is directly used as input for the PACE protocol and *PI** compared to the *PI* reference in the secure internal memory of the chip. If a terminal wants to calculate *PI** it needs *AD*, which is printed on the data page of the eMRTD in form of a 2D barcode. On the one hand this prevents tracking via the wireless channel with *AD*, and on the other hand a terminal needs optical access to the eMRTD data page to receive *AD*, which links the physical document to the chip. The most interesting part of [4] for this article is the discussion to replace EU EAC, the Country Verifying PKI, and the fingerprints in data group 3 with BioPACE V2, and a biometric template stored inaccessible in the eMRTD chip's internal secure memory. The authors identify several benefits e.g.: (1) Faster verification, due to the no longer existing requirement to transfer the raw

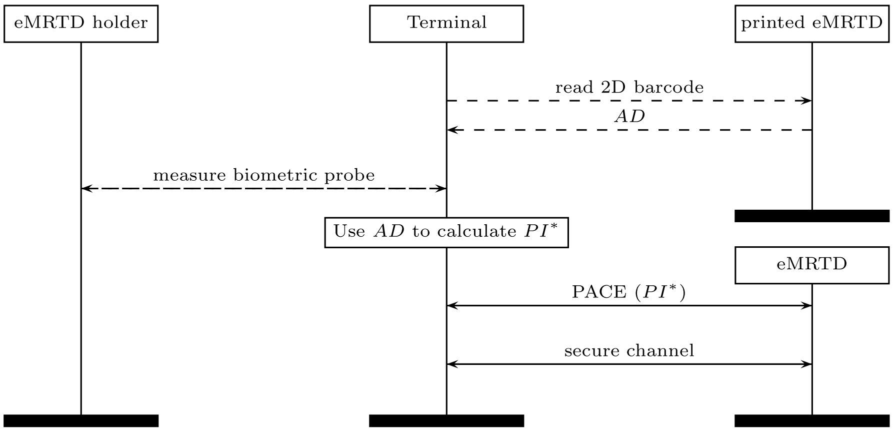

Fig. 1. The BioPACE V2 protocol.

fingerprints from the chip to the terminal, and the removal of the certificate chain validation on the chip. (2) Improved privacy, due to the removal of the raw fingerprints from DG3 with a biometric template, which is stored in the eMRTD's internal memory and therefore only accessible by the chip. (3) Decreasing infrastructure costs, because if Terminal Authentication is dropped, there is no more need to maintain the complicated Country Verifying PKI. In contrast to the benefits, the authors also identify some downsides of their approach e.g.: (1) The layout of the data page has to be changed, as well as the creation and enrolment process to print *AD* as 2D barcode on the data page. (2) BioPACE V2 only provides a coarse-grained access control mechanism, compared to the fine-grained access control of EAC for every data group. It establishes basically one of two access levels, because BioPACE V2 either grants complete access to the chip's data groups or no access at all. The authors diminish this downside with the fact that after removing the fingerprints from the chip, it contains actually no more sensitive data groups, which justify a complicated and expensive but flexible access control mechanism. In contrast to many other proposed eMRTD protocols from the scientific community the BioPACE V2 protocol is based on an already established protocol, the PACE protocol. We think it is more realistic that EAC could be replaced by a concept, which uses a protocol already established in the eMRTD domain as its basic building block, instead of a new completely self-created protocol. Therefore we will add BioPACE V2 to our evaluation and compare it to our proposals and the Hoepman protocol.

Pasupathinathan et al. [28] present a self-made protocol called On-line Secure E-Passport Protocol (OSEP Protocol). The authors claim to solve weaknesses of EAC. The OSEP protocol drops the access control flexibility of EAC and a terminal sends private information from the eMRTD to the country's embassy. In contrast to Pasupathinathan et al. [28] we think that both facts raise privacy concerns: a terminal, which needs access to the document holder's name stored on the chip, should not automatically get access to the sensitive fingerprints. Furthermore countries, which may track travellers through their embassies, is a show-stopper for any travelling privacy. Comparable to [13] we do not think that another self-made protocol is needed where no practical experience data exists how the protocol performs in practice. We also do not consider it realistic that the EU will drop EAC, because of a practically untested, self-made protocol. With these characteristics, the OSEP protocol disqualifies itself and we will not evaluate it against our proposals, BioPACE V2 and the Hoepman protocol.

3. Verifying public key infrastructure

This section introduces the purpose and hierarchy of the Verifying PKI. It has its own distinctive purpose. Without an additional mechanism there is no limitation who is allowed to read out the chip's data, if a third party gets hold of the physical document, regardless whether the document was handed over willingly, or an attacker obtained physical possession without the bearer's approval. To limit the access to the sensitive biometric data only to selected authorities, a PKI is needed to grant and validate the access rights of the inspection systems, the so-called Verifying PKI. It is well described in [30].

The evaluation of the access rights and validation of the authenticity from the terminal certificates has to be done by the eMRTD chip itself. Therefore the Verifying PKI uses card-verifiable certificates [22] to speed up the process. This process is called Terminal Authentication which is part of EAC.

The Verifying PKI structure can be seen in Fig. 2. The hierarchy of the PKI is as follows. Every country has a Country Verifying Certificate Authority (CVCA) which holds a self-signed certificate. The CVCA's task is to certify Document Verifiers (DV) by signing their certificates with the CVCA Private Key. A CVCA does not only sign domestic DV certificates, but also foreign DV ones to grant access for other member states to the eMRTD issued by the CVCA's state. Therefore a DV needs one certificate for each country that issues an eMRTD with EAC. There can be multiple DVs for every country.

As trust point the CVCA certificate of the issuing country is stored on every eMRTD chip with EAC support. Below the DV hierarchy level is the level of the terminals with their terminal certificates also called inspection system certificates. Terminals which need access to the sensitive data of eMRTDs from different countries need a certificate for each country granted by their DV.

For issuing the terminal certificates the DV does not need to contact every country itself, but instead every country maintains a so-called Single Point of Contact (SPOC), which is responsible for transnational communications and cross-border

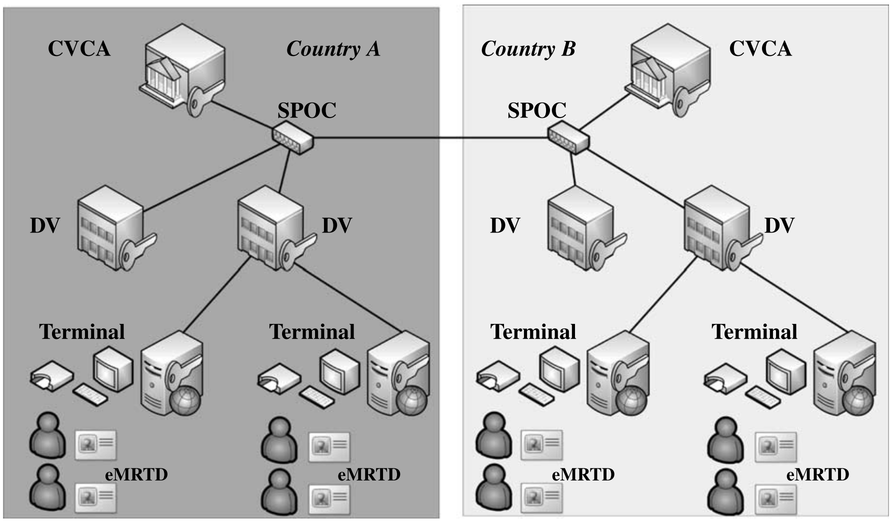

Fig. 2. The Verifying PKI and SPOC.

certifications. Each country that issues an eMRTD with EAC support or wants to read an eMRTD needs its own SPOC. The protocols of the SPOC for operations across international borders have to handle the following use cases [7]:

- “A DV wants to send a certification request to a foreign CVCA.”
- “A CVCA wants to send a issued certificate to the requesting DV.”
- “DV and CVCA can request a list of valid certificates needed to read an eMRTD.”
- “General messages can be exchanged between the national Verifying PKIs.”

These operations are specified together with two designated operation channels. The first is based on a web service interface and the second on manual exchange of removable media like USB storage devices, CD-R, DVD-R media, or publication on the Internet. The web service is protected by at least TLS v1.0 [20] with Client and Server authentication. The manual out of band communication through diplomatic means specifies the structure of the exchanged media and which metadata has to be provided in form of hash values for the transported data.

4. Shortcomings of Verifying PKI and solution candidates based on Internet domain protocols

In Section 4.1 we first address the shortcomings of the Verifying PKI, i.e. the missing revocation mechanism and the missing time source for an eMRTD. Once we have identified the drawbacks we discuss in Section 4.2 solution candidates based on Internet protocols to improve the Verifying PKI. The solution candidates from the scientific community have already been discussed in Section 2. Therefore these mechanisms will not be part of this discussion but will be evaluated together with the results from this section in Section 5.

4.1. Shortcomings of the current EU EAC implementation

Although the new protocols specified by the EU EAC standard [6] are sophisticated and thus enhance the security of former protocols, the current EAC standard still offers two unsolved weaknesses. They are linked to the new Verifying PKI and the associated Terminal Authentication. First, the eMRTD has no access to a precise and authentic time source, so it cannot accurately validate if a terminal certificate is still valid. Instead a pseudo clock mechanism is used, which is described below. The second problem is that a certificate once issued stays valid until the expiration date no matter what happens. So no actual revocation mechanism is present, but instead to limit the value of a stolen inspection system the issued inspection system certificates have a very short validity period, usually only one day. On the one hand this creates an enormous effort with respect to both generation of key pairs/certificates and their distribution and on the other hand this strategy does not provide the same security

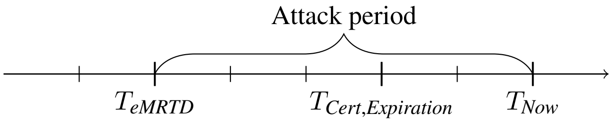

Fig. 3. Timeframe for attack.

level as a revocation, because of the pseudo clock mechanism an expired certificate can still be accepted as valid.

As announced above the missing time source is replaced by a pseudo clock mechanism, which works as follows:

The eMRTD stores a date T_{eMRTD} in an internal register which gets updated during the Terminal Authentication. Initially T_{eMRTD} is set during the chip personalization to the personalization date.

During the Terminal Authentication the eMRTD reads the “Expiration date” $T_{Cert,Expiration}$ field from all certificates and validates that $T_{Cert,Expiration}$ is not before T_{eMRTD}.

After every successful Terminal Authentication the eMRTD chip reads all certificates from the chain and checks which got the latest “Effective Date” $T_{Cert,Effective}$ field, which is the equivalent of the “Not Before” field from X.509 certificates. If $T_{Cert,Effective} > T_{eMRTD}$ then T_{eMRTD} is set to $T_{Cert,Effective}$ and stored in the internal register [6,30].

The problem which arises is that the eMRTD chip can only detect a past $T_{Cert,Expiration}$ value if it is used often, because then T_{eMRTD} is relatively accurate. Nevertheless an eMRTD chip cannot be sure if a terminal certificate is really still valid, because if $T_{eMRTD} \leqslant T_{Cert,Expiration} < T_{Now}$ the eMRTD will not detect an expired certificate. The possible attack period is shown in Fig. 3. So for a successful attack the attacker must already have a valid certificate and he can expand the time period in which his terminal can read biometric data. This only works if the eMRTDs chip gets no accurate time update from another terminal.

Possible reasons why the eMRTD got no clock might be explained from the problems that arise if you try to integrate a clock into an eMRTD, e.g. the missing power source.

4.2. Solution candidates to introduce revocation based on established Internet protocols

As of today, the Verifying PKI neither supports CRLs nor OCSP [5]. Although the reason is not given in [5] we believe that it is due to the missing external connection of the eMRTD and memory restrictions on the eMRTD. Computing power increases through progress and the next generation of smart cards will support TCP/IP, therefore these are no more obstacles [24,29].

In the following subsections we present potential Internet domain solution candidates to introduce a revocation mechanism to the Verifying PKI and discuss the

Table 1

Internet domain candidates and criteria

Criteria	Candidates		
	CRL	OCSP	SCVP
Storage requirement	High	None	None
Memory requirement	High	Low	Low
Computational amount	High	Low	Low
Network traffic	High	Low	Low
Real-time revocation	No	Yes	Yes
Permanent connection	No	Yes	Yes

practical feasibility, respectively. Our starting point are protocols, which are standardised for the Internet domain and thus thoroughly investigated.

Table 1 shows the three Internet domain candidates and their distinguishing characteristics as described in detail in the following sections.

4.2.1. Certificate Revocation List (*CRL*)

Certificate Revocation Lists (CRL) provide a mechanism to invalidate certificates before their actual expiration date. A reason for such an action can be e.g. the compromise of the private key or the release of a superseded certificate [18]. Besides completely revoking a certificate, a certificate can be put temporarily on hold until circumstances are clarified and the certificate can resume its validity period or become completely revoked. CRLs are specified in [17] as part of the X.509 PKI standard [18]. The CRL is a signed list of the revoked certificates and must be issued periodically by the Certificate Authority (CA). The CRL has a validity period itself and must be updated after the expiration. An advantage compared to other revocation techniques is that after the CRL has been received no more external connection is necessary until the CRL expires. One key problem with CRLs is that their size increases monotonically, sometimes it grows arbitrary large after some time [35]. The bandwidth and storage requirements make CRLs not attractive for low memory and limited processing power environments. Instead of full CRLs the delta variant may be used in conjunction with the delta CRL extension to reduce bandwidth usage, but the required storage problems remain or even become larger, through overhead [32].

In the context of the Verifying PKI a CRL has to be provided by the issuing country of the eMRTD, because a member state will not delegate this privilege to other member states. If the CRL is signed by the CVCA it can be verified with the certificate stored on the eMRTD chip. However, the eMRTD would need extra internal persistent memory to save the CRL. To check if it needs to download a new CRL the eMRTD chip would still need a clock. Without a clock the eMRTD chip needs to download the entire CRL during every Terminal Authentication. Depending on the size of the CRL this might be significant overhead and could immensely extend the validation time. Downloading the CRL would be the duty of the inspection system. Parsing through a big revocation list might also take unnecessary long for the eMRTD chip [35].

4.2.2. OCSP

The Online Certificate Status Protocol (OCSP) provides an alternative to CRLs [16]. Besides real-time status OCSP provides the benefit of lower bandwidth usage per request and no storage requirement compared to a CRL. Some OCSP responders present data simply fetched from a CRL, which results in an easy implementation, but is not better than the CRL in term of real-time revocation. CRLs should be avoided as direct data source and a modern database should be used instead to provide actual real-time revocation. A drawback is that the OCSP responder has to be available all the time [35].

Using OCSP as revocation mechanism in the Verifying PKI delivers many benefits over traditional CRLs. The eMRTD chip does not need additional internal memory for storing the list, the download size is smaller and simultaneously the eMRTD chip does not need to process an entire list of CRL entries. The eMRTD chip can get a direct response if the certificate has been revoked or is valid depending on its regular expiration date. Even so [9] has a different focus it favours OCSP to improve EAC. A time source is still needed, because the OCSP responder does not check the validity period of the certificate, but instead if it has been revoked (blacklist) and with the OCSP extension CertHash [2] also if the certificate has really been issued by the CVCA (whitelist). In our use case the validity period of the certificates will be verified by the eMRTD as part of Terminal Authentication and the OCSP responder should only send the status “good” (not revoked) or “revoked”. The “unknown” status is prohibited. For further evaluation and security discussion we assume an OCSP responder, which mimics this behaviour, uses the CertHash extension, and is supplied by a database which can be updated in real-time.

4.2.3. SCVP

The Server-based Certificate Validation Protocol (SCVP) in contrast to OCSP provides a server based full validation of a certificate, with optional revocation [19]. The complete certificate path creation, validation and check for revocation is done by the SCVP server. If the client trusts the server it can delegate nearly the complete PKI overhead to the SCVP server. This enables the use of a PKI for low-end devices. To check the validity status of a certificate the SCVP server uses either CRLs or OCSP. SCVP is not widely used yet, but has been tested on smart cards [27]. SCVP provides authenticity and integrity of the request and response messages, but does not ensure confidentiality. However, the SCVP standard suggests to use the Transport Layer Security Protocol (TLS) if confidentiality is needed [20].

An eMRTD chip with support for the SCVP would not only benefit from the features of OCSP, but would also no longer depend on a clock. SCVP messages would be signed by the CVCA (or a dedicated SCVP service) and SCVP also provides measures against replay attacks. Despite the need for a transport protocol between inspection system and eMRTD chip, because of the missing Internet connection, SCVP is a promising solution with regard to benefit and created effort.

4.3. Conclusion on the Internet based solution candidates

For a revocation it is mandatory that the eMRTD chip can securely communicate with a trusted home server. This is not possible without extra infrastructure to handle the requests and the willingness of the inspection system to play the role as a network bridge between the Internet and the current simple smart card communication protocols. Due to the availability of UMTS or LTE this assumption even holds for mobile inspection systems. Mobile inspection systems without Internet access can fall back to the validation of the physical security features, face recognition or a manual validation with the picture printed on the data page. OCSP and SCVP both provide good solutions if the infrastructure obstacles (i.e., the high availability demands) can be handled. Both protocols effectively solve the problem of stolen terminals and their efficiency has been proven in other domains. The classical CRL is not suitable for the EAC revocation, because of the low-power eMRTD chip (see Table 1).

5. Evaluation of all solution candidates

This section introduces an evaluation scheme and applies it to NTP in combination with OCSP, SCVP, the Hoepman protocol [13], and BioPACE V2 [4]. NTP together with OCSP will from now on referred to as NTP+OCSP. The criteria are mostly based on the well-known Software Engineering non-functional requirements [34].

Security is the first criterion which the candidates are evaluated against. This criterion consists of the resistance against certain attacks like replay attacks, and man-in-the-middle attacks.

Convenience and Acceptability are the next criteria which reflect the end user's benefits and drawbacks which the respective solution provides.

The *Total Cost of Ownership (TCO)* is a criterion which not only depends on the new technology needed to provide the services, but also on the reusability of existing IT structures.

If another country wants to introduce a new technology and therefore the global number of users changes dramatically, then *Scalability* is the criterion which considers this.

The fifth criteria are *Reliability and Availability* which rate the dependence on other systems and if the systems are loosely coupled or if they heavily rely on other components.

Feasibility is the last criterion which also includes how likely it is that a certain technology will be integrated into an eMRTD.

Some criteria are not independent e.g. the scalability can influence the availability and therefore the user's acceptance and so on.

In the eMRTD domain we consider *Security* and *Scalability* the most important criteria. On the one hand security is an absolute must, because of the embedded biometric data and on the other hand scalability is very important, because in tourist seasons the passengers boarding airplanes can increase drastically and smooth operation of inspection systems must still be ensured. A higher security level at border checks is one of the main reasons why eMRTDs were introduced in the first place. Therefore security is also one of the key factors for extending the current procedures. Another key factor why eMRTDs were introduced is the automation of border checks with so-called Automated Border Control gates (ABC gates) [12]. ABC gates can only make border checks faster if the underlying system properly scales with severe load scenarios like the vacation period. Therefore *Security* and *Scalability* will weight double for the final score.

For every criterion the candidates are rated positive (+), neutral (○) or negative (−) and for the final rank the individual ratings get points, these are then summed up to receive an end result.

5.1. Security

In this section all candidates are evaluated for potential weaknesses against common security attacks like replay attacks, and man-in-the-middle attacks.

The first item is the resistance against replay attacks. NTP, OCSP and SCVP all provide nonce support to individually link the unique request/response pairs, by default or via a protocol extension. The lightweight OCSP profile [10] should not be used, because it removes the nonce in favour of better scalability which is achieved by response pre-production and response message caching. To prevent replay attacks unique request/response pairs are essential.

Next topic is the resistance against man-in-the-middle attacks. NTP, OCSP and SCVP support the use of digital signatures for authenticity and therefore prevent man-in-the-middle attacks. Independent of the supported mechanisms, there is no direct use case for a man-in-the-middle attack, because confidentiality is no security goal, due to the fact that all time information and the revocation status are not considered confidential. A possible attack would be an Impersonation Attack in which the attacker tries to make the client believe that he is a legitimate server. This attack is also prevented by the same mechanisms as the man-in-the-middle attack.

A general security concern might be the introduction of TCP/IP itself, because it might open new attack vectors to the eMRTD. This can easily be mitigated by only allowing a one to one connection between the inspection system and the eMRTD with exactly one open socket. So with this careful design decision both protocols will provide a higher security increase than potential TCP/IP flaws a security decrease. Also future eMRTDs supporting IP will most likely not communicate to the Internet directly, but always with assistance of the terminal as proxy to handle network subtleties like DNS or routing, which also makes implementation of complex network details easier and more robust. OCSP, the Hoepman protocol and SCVP specify TCP/IP as their default transport layer protocol. Even so a different transport layer protocol might be chosen, for a fair rating we assume that all application layer protocols rely on the same transport layer protocol TCP/IP. Therefore this will not influence the rating.

From a security point the candidates from the Internet domain have no significant weaknesses. On the one hand the fact that NTP+OCSP consist of two different protocols whose services must be provided by two different daemons, even if they are running on the same server, provide two potential weak points and SCVP only one. On the other hand could the independence of both services also be treated positive, because it might be harder for an attacker to disturb both services. So this depends on the actual implementation and should not influence the rating. Therefore both Internet domain candidates get a positive security rating.

For the *Security* criterion the Hoepman protocol only defines resistance to replay attacks as a boundary condition, but this should not be a practical problem, because comparable to SCVP this could be achieved with a unique request/response pair by nonce support. As second requirement the Hoepman protocol creates an authentic channel from the chip to the back office. Since both entities have a common root certificate setting up such a channel is possible with common cryptographic primitives and such a channel is also resistant against man-in-the-middle attacks. Therefore the Hoepman protocol gets a positive rating.

BioPACE V2 consists of the BioPACE V2 pre-step and PACE itself. For the biometric pre-step no communication between the chip and the terminal is necessary. So the security against common attacks solely depends on the resistance of PACE against these attacks. The PACE protocol has been formally proven in [1], is considered secure against these attacks, and therefore BioPACE V2 also gets a positive rating.

5.2. Convenience and Acceptability

The user's convenience directly influences the acceptance of a certain technology. So a criterion must be how the new protocols influence the average border check time. A main benefit from the new protocols is better data privacy for the biometric data stored on the eMRTD.

The solution candidate's influence, on the border check processing time, shall be the first item for evaluation. The NTP+OCSP solution has the disadvantage that it can only lengthen the eMRTD evaluation, because the EAC verifying card-verifiable certificate chain must still be validated by the chip and the additional steps for time acquisition and the certificate revocation cost additional time irrespective of how much. The SCVP solution can make the evaluation process shorter, require the same amount of time or even could take longer.

For SCVP the certificate chain validation itself will take a shorter time, because the SCVP server has more computation power than a small smart card microprocessor. Two new potential time additions come to the verifying process on the SCVP server compared to current verification on the eMRTD. These are the acquisition of an accurate time and the certificate revocation mechanism. Both can be done independent of the certificate verification if NTP and automatic CRL download is used by the server. If OCSP is used by the server it would negatively influence the validation time and therefore a CRL should be preferred. We expect the SCVP validation process to be faster than on the chip and the only variable remaining is the transmission of the request and response.

Calculating an exact transmission time is not possible, because it depends on at least the bandwidth and the distance to the home SCVP server.

The next item of consideration shall be how the data privacy benefits from the solution candidates. NTP+OCSP and SCVP both provide the same benefit that expired terminal certificates will always be rejected and that stolen or compromised terminal certificates can be revoked effectively. Both mechanisms provide the same benefit, but one question is if the protocols could leak private information or enable tracking of the document holder. Neither NTP, OCSP nor SCVP send travel document specific data to the home server. NTP does not send any privacy relevant data at all and OCSP/SCVP send only data identifying the inspection system to the home server. Therefore the only negligible privacy concern is that the home server's operator could learn that one of the country's million passports is currently presented to the terminal. The operator is not able to identify the document holder any further and therefore we do not consider this a privacy risk.

So NTP+OCSP and SCVP only provide a benefit and pose no risk to the document holder's data privacy. Both Internet based solution candidates can provide convenience for the users and therefore boost their acceptance. NTP+OCSP provides all the benefits that SCVP does, but can only slow down the border check handling therefore it gets a neutral rating and SCVP a positive rating.

The Hoepman protocol is very similar to SCVP in regard to the fact that it delegates the certificate checks to a trusted third party server in the back office of the issuing country. Thus the Hopeman protocol is expected to provide a faster validation process than the current EAC Terminal Authentication, comparable to SCVP. Since the Hoepman protocol only sends the terminal certificate to the home server, the privacy concerns are as negligible as with SCVP. Therefore the Hoepman protocol gets a positive rating for *Convenience and Acceptability*.

In our analysis we identify that neither NTP, OCSP, SCVP nor the Hoepman protocol send travel document specific data to the home server. Nevertheless if the transferred data must be considered confidential due to possible regulations this additional security goal can be achieved by using TLS. The impact of the confidential transport channel is equal for all protocols and will therefore not influence the evaluation results.

The authors of BioPACE V2 [4] discuss in detail why the protocol provides improvements for border control check speed and data privacy. The speed up results because of the facts, that no more certificate chains have to be checked on the chip, and no more fingerprint images have to be transferred from the chip to the terminal over the wireless channel. The later fact also improves data privacy, as well as the fact that the introduced protected biometric template never leaves the chip. BioPACE V2 does not rely on external entities which could be a privacy threat. With these properties it is save to give BioPACE V2 a positive rating.

5.3. *Total Cost of Ownership* (*TCO*)

This chapter focuses on the expense necessary for the solution candidates. First the necessary new hard- and software will be assessed. Furthermore it is important which components of the already existent system can be reused or integrated directly or indirectly for example after a firmware update.

NTP, OCSP and SCVP have a relatively equal impact on the eMRTD PKI and inspection system structure. The eMRTD chip is not upgradeable via a firmware update, so only the next generation of eMRTDs could support the new protocols. If the current chip is powerful enough to perform all three protocols is hard to tell, but all of them have already been implemented on a regular smart card [27]. The current eMRTD chip is powerful enough to validate card-verifiable certificate chains, so it should be powerful enough to handle a time stamp package and an OCSP response or an SCVP response. Also neither of the protocols need any additional persistent storage space. So the financial impact on the eMRTD itself should be minimal from a hardware perspective. The software has to be changed of course to support the new protocols.

The next items to evaluate are the changes necessary to the inspection systems. The necessary modifications for the inspection systems operating system should be patchable with a new firmware. So only development costs occur, but no hardware upgrade costs. For NTP+OCSP and SCVP an Internet connection is necessary to communicate with the respective home server. The inspection system must already communicate with its DV and this DV must communicate with its country's SPOC. So some sort of network connection should already be present. Upgrading the broadband connection for the inspection system might be necessary as well as an upgrade for the SPOC to handle real time requests.

The last item for potential upgrade costs is at the home server. NTP+OCSP and SVCP need some sort of home server for every issuing country with a connection to the country's SPOC. The server must provide an NTP server and an OCSP responder or an SCVP server. To provide authenticity and integrity all three protocols support the use of digital signatures. The generation of the signatures could be accelerated by using Hardware Security Modules (HSM). Standard CPUs are also needed to handle the protocol request and the certificate chain creation and revocation for OCSP.

Even without exact figures SCVP and NTP+OCSP can be compared. On the one hand NTP+OCSP cost two HSM runs for digital signature generation because they are two stand-alone protocols and SCVP only one, but on the other hand SCVP needs more CPU time for the certificate chain building, revocation and verification, than NTP+OCSP for a revocation and system clock lookup.

The bandwidth consumption of NTP+OCSP and SCVP should be minimal for both. NTP+OCSP might have higher development costs for the eMRTD chips software, the inspection system software and the SPOC's software. The development costs should be minimal compared to the required hardware costs for the home server. As already mentioned above, NTP+OCSP might require more HSM signing runs and less CPU power, then SCVP. For the actual NTP+OCSP specification it could be considered to drop the internal signatures and instead sign both responses together in one big response block. With such an optimisation only the CPU time remains, which is much higher per SCVP request than per OCSP request. So NTP+OCSP gets a neutral ranking and SCVP a negative ranking for the TCO, because of the higher CPU time costs.

As discussed before, from a technical standpoint the Hoepman protocol is very similar to the SCVP protocol. Even though it is not specified in detail it is reasonable to assume that the financial impact of the back office server is comparable to the SCVP server. Since it additionally manages dynamic access rights and is based on a practically untested and unoptimised protocol the *TCO* might be even worse than for SCVP, which already got a negative rating. So the Hoepman protocol also gets a negative rating.

BioPACE V2 comes with negative as well as positive changes in context of the *TCO*. On the one hand the layout of the standardised data page, as well as the enrolment and personalisation process have to be changed, because *AD* needs to printed on the data page as 2D barcode for BioPACE V2. On the other hand the maintenance costs of the Country Verifying PKI can be omitted because it is not needed any more for BioPACE V2. Terminals also need no constant connection to other components, because BioPACE V2 needs no external components. We consider the financial impact of dropping the Country Verifying PKI higher, than the impact of changing the layout and therefore BioPACE V2 gets a positive rating for the *TCO*.

5.4. Scalability

Scalability describes the system's behaviour if the requirements on supported user clients change drastically. The increased input can influence the performance, because of higher resource requirements which depend on the complexity of the entire system. One criterion to evaluate is the load per request, which directly influences the system's scalability. The load on the home server and on the network between inspection system and home server can be differentiated.

To compare the network load of NTP+OCSP with the one from SCVP it must be taken into consideration that the protocols will most likely be implemented in a more lightweight form. The NTP network impact is minimal and therefore only OCSP and SCVP shall be compared. All certificates must be checked for revocation in case of OCSP. In case of SCVP all certificates need verification. The requests could contain all necessary certificates or just the serial numbers of the certificates which would result in a lower network usage.

For OCSP the serial number is always enough, because even if the OCSP responder does not know the associated certificate for the serial number, the certificate revocation status is considered good.

For SCVP a serial number certificate look up must always provide a result, because otherwise no verification of the complete chain is possible. The SCVP server can be easily provided with the CVCA certificate because it is present in the same country. The DV certificate's signing requests are all handled by the SPOC which shall also be connected to the SCVP server. Therefore an automatic supply of DV certificates should also be possible without requiring major effort. One problem however lies in the acquisition of the terminal certificates. They are created by the DV, for every terminal, on a daily basis and the serial number remains unknown for the SCVP server. So for SCVP the terminal certificate must be sent entirely instead of just the serial number.

SCVP would have a higher average bandwidth usage than NTP+OCSP. For the TCO scoring, it was already estimated that SCVP would have a higher CPU load per request. Therefore NTP+OCSP gets a positive rating and SCVP a neutral one.

For the Hoepman protocol a transfer of the certificate is also always necessary, which makes the network impact higher than the impact of NTP+OCSP. Compared to SCVP it is an untested and unoptimised protocol, which therefore either performs similar to SCVP or worse. A difference to SCVP is that the back office server sets the access rights dynamically, which is in theory a nice feature but costs higher CPU load per request because of the decision logic than SCVP. Therefore the Hoepman protocol gets a negative rating compared to the optimized and well-established Internet standards.

The *Scalability* of BioPACE V2 is very easy to discuss, because it does not rely on external components, which could be a potential bottleneck. The number of BioPACE V2 executions per minute is simply limited by the number of terminals at a border control station and not by some remote issuing country component. Therefore BioPACE V2 simply scales linear with the number of terminals independent of external components and therefore gets a positive *Scalability* rating.

5.5. *Reliability and Availability*

Reliability and the linked availability are influenced by the solution candidates complexity and the resulting points of failure. A terminal not supporting the protocols or even a broken terminal always breaks the regular border control procedure and is out of scope for this evaluation. NTP+OCSP and SCVP need an Internet connection to communicate with the home server. If the connection fails, all three protocols will not work. They also need the verifying country and issuing country SPOC to be online at all times. Both are points of failure as well as the home server of the issuing country. On the home server runs the NTP and OCSP daemon or the SCVP daemon to process the requests from the eMRTD. All of these are potential points of failure.

One small difference here is that for NTP+OCSP two daemons could stop working and for SCVP only one, but again the purpose of NTP and OCSP is independent, so one service still running from two could also be considered as a better circumstance than a complete breakdown of a single service.

NTP+OCSP and SCVP have no big difference in their points of failure. It could be argued that the tasks of SCVP are more complicated and more prone to error, but this would involve potential implementation errors which are out of scope. Both candidates heavily rely on external systems and therefore both get a neutral rating.

The Hoepman protocol also relies on an external component, the back office server. As untested and more complex protocol (due to the dynamic access rights) the reliability can be considered worse or equal to SCVP. For NTP+OCSP and SCVP we did not consider potential implementation errors and defined them as out of scope. Therefore the Hoepman protocol gets the same neutral rating as SCVP, because it also heavily relies on external systems.

For the BioPACE V2 protocol the only risks are a terminal not supporting the protocol or a broken terminal, but we defined these scenarios as out of scope, because they are protocol independent. Impacts due to failure of an external system do not exist for BioPACE V2, because it does not rely on external systems. So it gets a positive rating for *Reliability and Availability*.

5.6. Feasibility

Feasibility for the solution candidates can be divided into technical feasibility, financial feasibility, economical feasibility and the basic conditions concerning the existing infrastructure.

From a technical perspective all solution candidates are possible. NTP, OSCP and SCVP were implemented for some research projects on smart cards and can therefore be considered as technical feasible on the eMRTD chip.

The financial part was already evaluated in, Section 5.3 therefore this shall not have an impact on the feasibility evaluation. The economical feasibility shall be the matter at hand. NTP+OCSP and SCVP both extend the European EAC mechanism and provide effectively the same benefit. Financial factors aside both candidates require a certain amount of development effort. NTP+OCSP are two protocols, but do not automatically lead to the doubled development effort, because the protocols are older, simpler and most likely more common to the developers for the implementation on a smart card. What sets the difference is that NTP and OCSP could be more or less directly implemented on a smart card with little or no development effort for the home server. SCVP in the eMRTD would need an implementation with a single request response pair and the missing access to the terminal certificates for the home server would enlarge the request or require more effort for the DVs. That is why NTP+OCSP are considered more likely with this simple analysis than SCVP.

SCVP needs a more complicated home server, the protocol would have to be adjusted and would create more burden for the DVs. Therefore NTP+OCSP gets a positive rating and SCVP a negative rating.

The Hoepman protocol is a theoretical concept and therefore it is only possible to speculate about its technical feasibility. It consists of common cryptographic primitives so it is very likely that it is technically feasible. From an economical perspective it is simply unlikely why the EU should select an untested new protocol, which provides no practical benefits compared to the competitors, instead of a well-established and tested protocol. This is why the Hoepman protocol gets a negative *Feasibility* rating.

Even so BioPACE V2 has not been implemented yet it is based on two well-established components. The PACE protocol, which is already used in the eMRTD domain and biometric template protection which has been implemented in many flavours in research projects. So from a technical perspective the protocol is clearly feasible. The economical perspective is a different story, because on the one hand the protocol relies on a well-tested, established standard, the PACE protocol. On the other hand there exists no internationally, openly standardised biometric template protection mechanism and the decision to completely shut down the established Country Verifying PKI is not an easy one to convince all EU member states, which already invested money in EU EAC. It is very hard to estimate the impact of such an extreme approach, even so it has clearly strong benefits. This discrepancy leads to a neutral rating for BioPACE V2's *Feasibility*.

5.7. *Evaluation result*

Table 2 shows a summary of the solution candidates evaluation results, and Table 3 presents the final results. The positive rating gets two points, the neutral rating one point and the negative rating zero points. Additionally the points for *Security* and *Scalability* will be doubled. BioPACE V2 ranks first with 15 points, NTP+OCSP

Table 2

Evaluation ratings

Criterion	NTP+OCSP	SCVP	Hoepman	BioPACE V2
Security (replay and man-in-the-middle attack)	+	+	+	+
Convenience and Acceptability (border check time, privacy)	○	+	+	+
TCO (hardware, software, reusability)	○	−	−	+
Scalability (network load, home server load)	+	○	−	+
Reliability and Availability (complexity, points of failure)	○	○	○	+
Feasibility (economical)	+	−	−	○

Table 3

Points and result

Criterion	NTP+OCSP	SCVP	Hoepman	BioPACE V2
Security (×2)	4P	4P	4P	4P
Convenience and Acceptability	1P	2P	2P	2P
TCO	1P	0P	0P	2P
Scalability (×2)	4P	2P	0P	4P
Reliability and Availability	1P	1P	1P	2P
Feasibility	2P	0P	0P	1P
Point sum	13P	9P	7P	15P
Final rank	2	3	4	1

ranks second with 13 points, SCVP third with 9 points and the Hoepman protocol last with 7 points. So the recommended solution by our evaluation is BioPACE V2 or NTP+OCSP.

6. Conclusion and future work

This article presented weaknesses and possible solutions for the current EU EAC implementation for eMRTDs. The problems of the missing accurate time and the linked terminal certificate revocation were explained and shown how they can be solved. A winner was found in the form of BioPACE V2 [4], but NTP with OCSP does only differ by two points and might be more feasible for adoption in the EU. [9] also favours OCSP and states that an authentication proof involving the home CVCA would be the ultimate trust mechanism for EAC. Nevertheless a great amount of new infrastructure would be needed for NTP, OCSP or SCVP, which would not be needed for BioPACE V2.

For future work both Internet domain solutions could be optimized to become more attractive by merging NTP and OCSP into one protocol without violating the standards, or stripping possible unnecessary overhead from SCVP.

BioPACE V2 is according to the evaluation the strongest proposal from the scientific community and builds together with NTP+OCSP one of the two best solutions to consider as improvement for the eMRTD domain.

Another topic for future discussion is the creation of an OCSP extension to carry the terminal access rights instead of encoding them into the terminal certificates. Either to override the access rights of a valid certificate or to completely outsource the access rights to the real-time OCSP. Which would be similar to the Hoepman protocol [13], but based on proven Internet standards.

For a look in the future to see which solution might become reality in a fourth generation of eMRTDs it depends on the specific future requirements of EAC, and if the effort for the terminal certificate revocation and the precise validation time can be justified, or if dropping EU EAC completely and replacing it by BioPACE V2 will be favoured.

Acknowledgments

This work was supported by the European Commission through the FIDELITY EU-FP7 project (Grant No. SEC-2011-284862) and CASED.

References

[1] J. Bender, M. Fischlin and D. Kügler, Security analysis of the PACE key-agreement protocol, in: *Information Security*, Lecture Notes in Computer Science, Vol. 5735, Springer, Berlin, 2009, pp. 33–48.

[2] H.-J. Bickenbach, J. Brauckmann, G. Alfred, T. Horváth and H.-J. Knobloch, Common PKI specifications for interoperable applications, v2.0, 2009.

[3] N. Buchmann and H. Baier, Towards a more secure and scalable verifying PKI of eMRTD, in: *EuroPKI 2013, 10th European Workshop on Public Key Infrastructures*, 2013.

[4] N. Buchmann, R. Peeters, H. Baier and A. Pashalidis, Security considerations on extending PACE to a biometric-based connection establishment, in: *2013 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2013, pp. 1–13.

[5] BSI, Certificate Policy für die ePass-Anwendung der hoheitlichen Dokumente, Bundesamt für Sicherheit in der Informationstechnik, 2010.

[6] BSI, Technical guideline TR-03110: Advanced security mechanisms for machine readable travel documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), 2.05 edition, Bundesamt für Sicherheit in der Informationstechnik, 2010.

[7] Česká technická norma, CSN 36 9791 ed. A – Information technology – Country Verifying Certification Authority key management protocol for SPOC, 2009.

[8] R. Chaabouni, Solving terminal revocation in EAC by augmenting terminal authentication, in: *2013 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2013, pp. 1–8.

[9] R. Chaabouni and S. Vaudenay, The extended access control for machine readable travel documents, 2010.

[10] A. Deacon and R. Hurst, The lightweight Online Certificate Status Protocol (OCSP) profile for high-volume environments, RFC 5019 (Proposed Standard), 2007.

[11] B. Deufel, C. Mueller, G. Duffy and T. Kevenaar, BioPACE – biometric passwords for next generation authentication protocols for machine-readable travel documents, *Datenschutz und Datensicherheit* **37**(6) (2013), 363–366.

[12] Frontex – European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, Best practice operational guidelines for Automated Border Control (ABC) systems, 2012.

[13] J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk and R. Schreur, Crossing borders: security and privacy issues of the European e-passport, in: *Advances in Information and Computer Security*, H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama and S. Kawamura, eds, Lecture Notes in Computer Science, Vol. 4266, Springer, Berlin, 2006, pp. 152–167.

[14] ICAO, MRTD Report, Vol. 1, No. 1, 2006.

[15] ICAO, MRTD Report, Vol. 2, No. 1, 2007.

[16] IETF, RFC 2560 – X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP.

[17] IETF, RFC 3280 – Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) profile.

[18] IETF, RFC 3820 – Internet X.509 Public Key Infrastructure (PKI) – proxy certificate profile.

[19] IETF, RFC 5055 – Server-based Certificate Validation Protocol (SCVP).

[20] IETF, RFC 5246 – The Transport Layer Security (TLS) protocol – Version 1.2.

[21] IETF, RFC 5905 – Network Time Protocol version 4: protocol and algorithms specification.

[22] ISO, ISO/IEC 7816-8: Identification cards – Integrated circuit cards – Part 8: Commands for security operations, International Organization for Standardization, 2009.

[23] ISO, ISO/IEC 24745:2011: Information technology – Security techniques – Biometric information protection, International Organization for Standardization, 2011.

[24] L. Kyrnitszke, T. Ravishankar and T. Violleau, Java Card 3 platform – white paper, Sun Microsystems, Inc., 2008.

[25] C.H. Li, X.F. Zhang, H. Jin and W. Xiang, E-passport EAC scheme based on Identity-Based Cryptography, *Information Processing Letters* **111**(1) (2010), 26–30.

[26] T. Moses, Protecting biometric data with Extended Access Control – securing biometric datasets in electronic identification documents, Entrust, Inc., 2010.

[27] K. Papapanagiotou, C. Markantonakis, Q. Zhang, W.G. Sirett and K. Mayes, On the performance of certificate revocation protocols based on a Java Card certificate client implementation, in: *SEC*, R. Sasaki, S. Qing, E. Okamoto and H. Yoshiura, eds, Springer, Berlin, 2005, pp. 551–564.

[28] V. Pasupathinathan, J. Pieprzyk and H. Wang, An on-line secure e-passport protocol, in: *Proceedings of the 4th International Conference on Information Security Practice and Experience, ISPEC'08*, Springer, Berlin, 2008, pp. 14–28.

[29] W. Rankl and W. Effing, *Smart Card Handbook*, 4th edn, Wiley, New York, 2010.

[30] T. Straub, M. Hartl and M. Ruppert, Digitale Reisepässe in Deutschland – Prozesse und Sicherheitsinfrastruktur, in: *Sicherheit*, J. Dittmann, ed., Lecture Notes in Informatics, Vol. 77, GI, Bonn, 2006, pp. 233–243.

[31] Technical Advisory Group on Machine Readable Travel Documents, TAG-MRTD/17-WP/11, Release 11, Final edition, International Civil Aviation Organization (ICAO), 2007.

[32] H.C. van Tilborg and S. Jajodia, eds, *Encyclopedia of Cryptography and Security*, 2nd edn, Springer, Berlin, 2011.

[33] S. Vaudenay and M. Vuagnoux, About machine-readable travel documents, *Journal of Physics: Conference Series* **77**(1) (2007), 012006.

[34] K.E. Wiegers, *Software Requirements*, 2 edn, Microsoft Press, Redmond, 2003.

[35] D.H. Yum and P.J. Lee, Separable implicit certificate revocation, in: *ICISC*, C. Park and S. Chee, eds, Lecture Notes in Computer Science, Vol. 3506, Springer, Berlin, 2004, pp. 121–136.