PKI Digital Signatures For Machine Readable Travel Documents

M. Auriga Herdinantio - 13506056

Informatics Engineering, School of Electrical Engineering and Informatics, Institut Teknologi Bandung

e-mail: au_hadetyozzz@yahoo.com

Abstract

Technology, have both changed the world dramatically in recent times. The resulting need for improved international security is also having a significant impact on the official identity documentation of individuals. Whereas counterfeiting of identity documents, and alteration of legitimate identity documents have always been a problem, The International Civil Aviation Organization (ICAO) has been developing standards for the next generation of passports, the latest version of which was released in October 2004. The most important change in these standards is the embedding of a contactless, smart card processor chip within the passport booklet.

The processor will be used to store specific biometrics of the document holder in addition to some personal information. The stored information can then be presented to border control officers at the time of travel. The new passport design is intended to serve two purposes: (a) the biometric information can be used for identity verification at border control, and (b) cryptographic technologies can be used to ascertain the integrity and originality of passports, thus preventing high quality passport forgeries that might otherwise pass a visual inspection.

This paper contains an explanation about application and usage of modern public key infrastructure (PKI) schemes for the implementation and use of Digital Signatures with Machine Readable Travel Documents ("MRTDs"). This use of PKI technologies and Digital Signatures is primarily intended to augment security through automated and selfcontained means of authentication of MRTDs and their legitimate holders. This paper also analyze ways and specific methodologies to implement such international MRTD authentication through Digital Signatures

Keywords : MRTD, Digital Signature, PKI

1. INTRODUCTION

The International Civil Aviation Organization (ICAO) is a specialized agency of the United Nations that promotes civil aviation, including setting standards for passports, visas and other travel documents.

In 2002 the U.S. Congress passed the Enhanced Border Security and Visa Entry Reform Act. Section 303(c) of that act requires that countries that participate in the US Visa Waiver Program have a program to issue machine readable passports that are tamper resistant and incorporate biometric and document authentication identifiers that comply with standards established by ICAO. In the interest of international reciprocity, the U.S. will issue similar machine readable passports to U.S. citizens.

In 1980, ICAO introduced the use of machine-readable data printed on the data page of passports with Optical Character Recognition (OCR) text. This OCR information called the Machine-Readable Zone (MRZ) consists of the document holder's name, date of birth, sex, the document's identification numbers and validity dates.

The next stage in machine-readable data was the use of 2-D barcodes. These can be used to encode ¼ 8000 bytes of information, and are in current use on many passports, visas, and driving licenses.

ICAO's standards for the next generation MRTD specify a contactless smart card microchip, conforming to ISO 14443, to be embedded within the passport booklet. These chips will be embedded along with their antennae, which, when brought into an appropriate electromagnetic field, will generate an electric current that can power the chip.

Contactless smart cards offer several advantages over contact smart cards,including no wear and tear of the physical contacts, faster data transmission rates, and not needing to change the physical appearance of a passport by adding electrical contacts. However, contactless smart cards have two potential disadvantages. Because the information is transmitted as radio-frequency signals, it may be possible for unintended recipients to intercept information. Second, if many contactless smart cards are physically close together, a reader will have difficulty sorting out which transmission comes from which card.

There have been multiple proposals to use the ICAO biometric passport technology for national identity cards and other purposes. The United Kingdom began with a proposal for a combined driver's license and passport that has

evolved into a full national identity card bill in Parliament.

However, the proposal has come under extensive debate, but it appears likely to pass as of the date when this paper is being written. Similar projects are underway in a number of countries, including Estonia and Singapore. The ICAO biometric passport technology might also be used for US driver's licenses to meet the requirements of the REAL ID Act of 2005, although no such requirement has been defined yet.

An important question is whether the ICAO specifications meet the intent of the US Congress in the Enhanced Border Security and Visa Entry Reform Act of 2002. The law itself does not give reasons for its requirements. Congressional intent can only be determined from the debates over the act. In this portion of the debate, it is clear that the Senate was most concerned about known terrorists not being detected when they entered the Unites States and that the 9/11 terrorists had overstayed their visas.

While the ICAO specifications may technically meet the needs of border crossing authorities, additional concerns arise in the deployment of the proposed technology. For example, the new technology may facilitate attack on security checkpoints other than those at border crossings.

Figure 1 Machine Readable Zone (MRZ)

2. DIGITAL SIGNATURE APPLICATIONS FOR MRTD

The application of Digital Signatures to MRTDs is accomplished through the following stages:

A. Digital recording of MRZ data. Although the MRZ already exists on the MRTD in machine-readable form, this data must be duplicated in the digital data storage area of the MRTD. This is necessary if the Digital Signature is to provide further protection for the MRZ data; any discrepancies between the OCR print and the digitized MRZ data would certainly raise an alarm at the border.

B. Digital signing of the digitized MRZ data. The MRZ data is hashed using standard algorithms to form the "MRZ digest" value, which is then encrypted with the appropriate private key of the issuing State. The resulting encrypted hash value, the MRZ's digital signature, is appended to the MRZ data to be recorded digitally on the MRTD.

C. On a paper-based or inked MRTD the digitized MRZ data with the Digital Signature is likely to be stored in the optional recording area as specified by 9303 standards, using a 2D bar code. These bar codes have limited storage space, perhaps 2000 bytes on a typical Part 1 data page. On more advanced forms of MRTD, the larger available data memory on these technologies (chip, optical memory) will be used to accommodate the digitized MRZ data and much more.

The Digital Signature on the MRTD can only be unscrambled by the corresponding public key of that issuing State, and that public key provides no information or help whatsoever in determining the companion private key that was used to encode the Digital Signature in the first place. As a result, short of serious espionage within the issuing State to reveal the private key, there is no opportunity for counterfeiters to forge or alter an MRTD since the Digital Signature will not match.

Incorporation of a biometric into this scheme provides significant additional security, in that it removes from criminals the ability to replace photos and other biometrics, since the photo and other biometrics are tied to the digitized data stored and protected by the Digital Signature. Even with a 2D bar code on a Part 1 document, a highly compressed photo image may be stored along with the MRZ data and the Digital Signature.

This will at least permit a 3-way inspection check involving the photo on the document, the digitized photo stored on the document, and the person appearing in front of the inspector. With the Digital Signature protecting the digitized data, photo substitution is not workable since the digitized (and Digital Signature-protected) photo must also be changed. The criminal in this case must resort to crossing a border as an imposter with a stolen or copied document.

The inclusion of biometrics is particularly significant where advanced forms of MRTDs are deployed, as the larger data storage areas available can accommodate sufficient biometric image and template sizes to enable automated or computerbased along with human inspection. Here the computer will provide another level of verification using facial recognition or other biometric comparison algorithms, to back up (or perhaps someday replace) the judgment of the

human inspector. In this case, even posing as an imposter is made very risky.

All of these benefits offered by a Digital Signature process for MRTDs take place at the border without necessary reference across international networks; in other words, once the public keys of issuing States are known, the verification process is carried out with the data and the Digital Signature on the MRTD only. This provides the necessary means to ICAO MRTD-participating countries to increase trust in such documents and the data contained on them without changing the stand-alone nature of border inspections or necessarily increasing the time required for them.

As a result, the incorporation of Digital Signatures to protect MRTD data is an important priority for the ICAO community. However, implementation of PKI infrastructures to carry this out, where security is paramount and where changing public keys of all issuing States must be shared with all other states, is not a trivial consideration.

3. METHODOLOGY AND INFRASTRUCTURE

Methodology each country is responsible for the generation of its own MRTD signing keys. These key pairs are to be maintained securely by each country, as described below, and are to be used for signing MRTDs issued by their MRTD issuing locations. The infrastructure uses a central MRTD authority in each country as the prime key generation and management site, essentially the root certificate authority for that country in issuing ICAO-format certificates for the MRTD signing application. This process is shown in Figure 2.

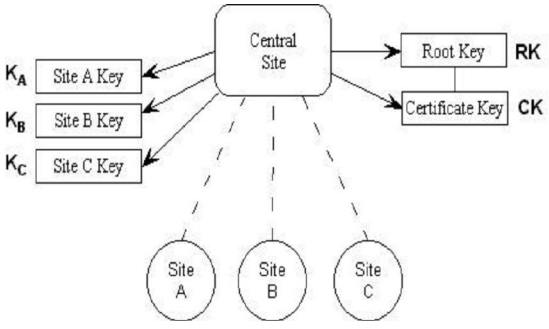

Figure 2 Central Key Generation In Each Country

In Figure 2, a country with 3 issuing (printing) sites is assumed for purposes of explanation. In this case, a key pair (Kn) is generated for each such site (although this is a matter for each country to decide, guided by ICAO recommended practices in this regard), but maintained in the central secure location.

In addition, to support the ICAO certificate infrastructure a root or master country key ("RK") is also generated, along with a "certificate signing key' ("CK").These latter key pairs are considered very secure and will not change very frequently, perhaps ever 5 years. This will be important for operation of the scheme.

The public key portion of each site-signing key (Kn) will be forwarded to ICAO as will be seen below. For basic MRTD signing purposes, the MRTD data to be signed at site A in each case, for example, is forwarded to the central site, which computes the Digital Signature value and returns the Digital Signature to the site for printing on the MRTD. This is shown in Figure 3 below.

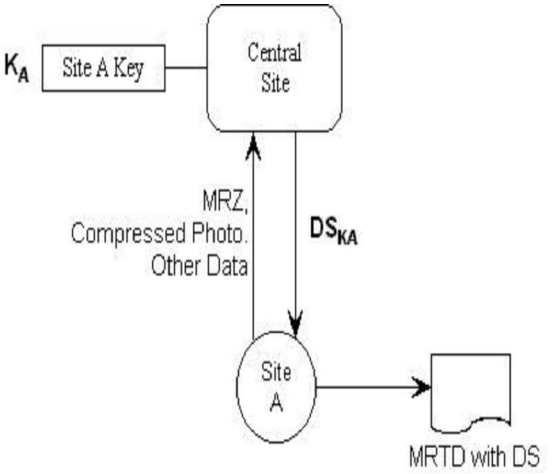

Figure 3 Basic MRTD Signing

The communications in this case will take place across secure communications facilities that will be required (and likely already in place) in each country. Importantly, however, the actual private key for site A is not released from the central location, which greatly simplifies the process and the cost of implementation in each country and also facilitates the trust that must be placed in the Digital Signature. Proper electronic security measures need only be implemented in one location.

Modern security technologies already offer substantial means of implementing such secure sites. The implementation of a Secure Key Management System (SKMS) for key protection, using special hardware devices and configurations to provide this security, are already widely in use. In particular the utilization of socalled Hardware Security Modules (HSM's) with appropriate input control security can provide a very high level of security for a country's private keys and hence for the utility of the application in the ICAO community. These HSM devices typically offer:

A. Physical and electronic protection for private keys generated and maintained, incorporating such strong features as active zeroization upon serious attempts at wrongful entry. The keys are extremely well protected;
B. Key generation for multiple sites and multiple types (of MRTDs, for example), through partitioning;
C. Fast signing without release of the private key by the HSM. Because of this the country configuration with central key management signing can be readily implemented with regular (secure) communications facilities;
D. Very secure entry/update restrictions, with such protection as multipleperson authorization for any update or change and robust individual identification standards. Many of these devices are validated to FIPS 140- 1 Level 35 specification or equivalent.

The Secure Key Management System and general country configuration is shown schematically in Figure 4 below.

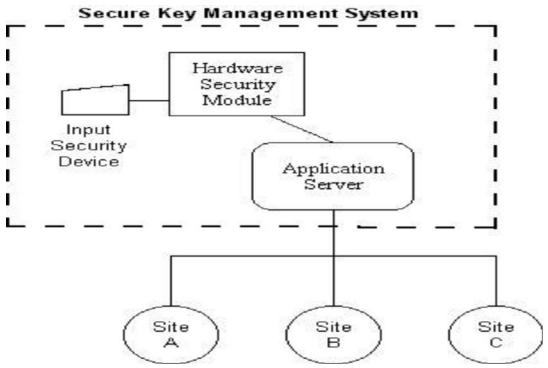

Figure 4 Schematic of a Country Secure Key Management System

The public keys corresponding to the country private keys so generated are communicated to ICAO, and to the world ICAO MRTD community, through the use of data contents and formats constituting an "ICAO PKI certificate".

These certificate formats will conform to accepted PKI standards such as ISO X.509 but with a simplified data content specific to ICAO requirements. These certificates will themselves be signed by ICAO acting as the de facto Registration Authority (RA) or Root CA in this regard, as part of its Directory and key dissemination service.

The methodology for the ICAO directory update service and signing mechanism is shown in Figure 5.

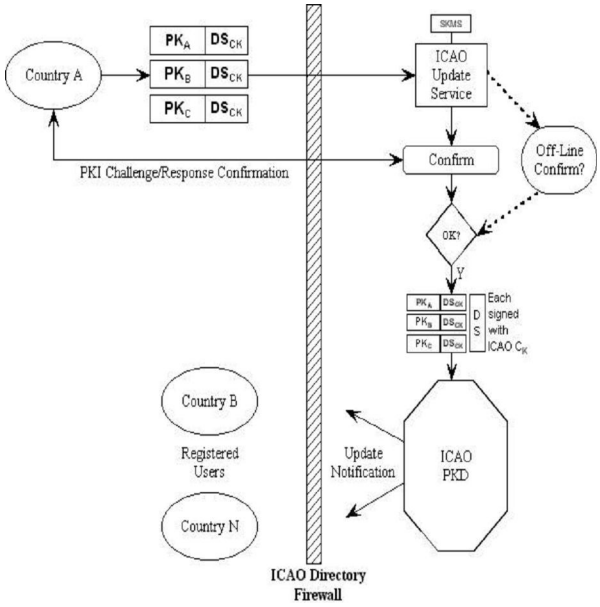

Figure 5 ICAO Public Key Certificate and Update Process

This diagram demonstrates how the certificate infrastructure will operate. It consists of several important components, as follows:

A. Country A (in this example) has generated three key pairs for each of its 3sites (A, B, and C) as in previous examples. To communicate the public key components of these key pairs, it composes ICAO-format certificates and signs each such certificate with its "certificate signing key" or CK (see Figure 2). This CK is very static and is known to all other ICAO member countries through a similar update mechanism upon enrollment in the MRTD Digital Signature program. In other words, while the public keys used by Country A to sign its MRTDs will change regularly, the public key certificates forwarded by each country to ICAO are signed by the country with its highly-secure and relatively unchanging CK.
B. These ICAO-format certificates are sent to the ICAO PKD Update Service. Upon receipt, it is proposed that the ICAO site automatically issue a confirmation process with Country A, which could operate like this:

- ICAO encrypts the information received using the public key (CK) of the sending country, and itself signs the whole message with the ICAO master private key. Note the proposed setup of a Secure Key Management System within ICAO itself for this purpose.
- Country A unscrambles the message using its private key CK, which only it can do, and, knowing the public portion of the ICAO master key, verifies the ICAO Digital Signature for the message to ensure that the message really came from ICAO and has not been altered. It then repeats the process using the ICAO public key

to encrypt the message and then sign it back with its own private key CK.

C. Upon receipt of this confirmation, and with no other suspicions that might warrant off-line confirmation with the country in question, ICAO then proceeds to update its public key directory with the new public key certificate information for Country A, signing each with its own private key to signify that the confirmation process has been successfully carried out. It then sends out an automatic notification to all member countries that such an update has occurred. The new Country A certificates are thereafter available on the directory.

Although it is true that the original message and information from the sender (Country A in this example) can be encrypted and signed by the sending country initially, it is proposed that the above confirmation step be incorporated for two important reasons, namely:
A. The sending country is thereby assured that ICAO has indeed received the message and that the information has not changed in any way from the original message sent;
B. ICAO is effectively relieved of any liability concerning the information it will store in the PKD, including inadvertent errors, since it has re-checked the information with the sending country, which has confirmed it. (Two of the benefits of this use of PKI for digital signatures are to verify that data has not been altered in any way, and to ensure that the originating country cannot later repudiate the message sent.)

It is also recognized that such challenge/response communications mechanisms will no doubt have been employed for security in the communications process itself, at the transport or other level, where session keys and other keys may be utilized. This however occurs more or less invisibly at lower levels of the communications hierarchy. It is considered important to have a similar process at the ICAO application level for proactive validation of keys and PKD integrity.

Key certificates are thereafter stored reliably on the PKD, and other countries accessing them will see them signed both by the originating country, using its secure CK, as well as by ICAO to indicate that the information has been properly confirmed and entered into the Public Key Directory service.

This is significant: an agent cannot penetrate the ICAO update site or facility and load improper keys for a country, since the agent will not have access to that country's signing key CK nor the ICAO private key also used to sign the certificates on the PKD Even physical attempts to break into the ICAO site will not work with the use of multiple authorization keys for any update and the physical impossibility of breaking open and stealing the secret keys from a proper HSM device.

This certificate infrastructure must be maintained at all times for the ICAO MRTD application, and will eventually apply directly to the issuance of certificates on advanced forms of MRTDs themselves, even though these advanced forms of MRTDs will have sufficient data space for the full ICAO PKI certificate. In other words, the role of ICAO and its directory service, acting as de facto RA for the global ICAO MRTD community, will remain an essential role.

The Digital Signature process applying to advanced forms of MRTDs is shown in Figure 6.

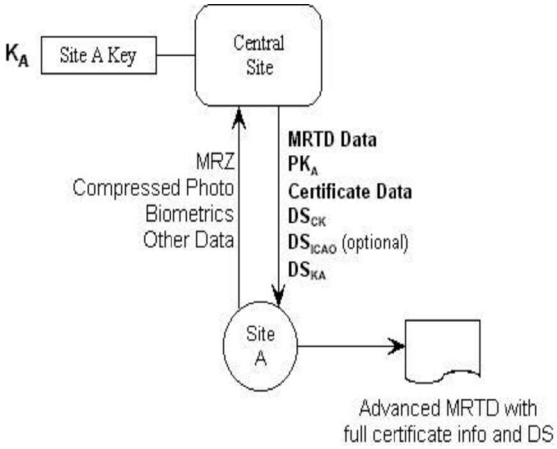

Figure 6 Future Signing of Advanced Forms of MRTDs

5. ANALYSIS AND COMPARISON PKI ALGORITHMS

There are a number of PKI algorithms in use and accepted today, but the main ones for use by states for these purposes are shown in the following, with their reference standards and performance characteristics

A. DSA, or Digital Signature Algorithm. This algorithm was developed for US Government digital signature use, and produces a digital signature of 320 bits (40 bytes). The algorithm must involve a public key of at least 1024 bits for adequate security for the foreseeable future.
B. RSA, or Rivest Shamir Adleman algorithm. This private sector standard is very strong and is considered somewhat "slow" in signing but fast in verification. It requires a minimum private key length of 2048 bits for security, which produces a digital signature of 1024 bits and requires a public key of 1088 bits.
C. ECC/ECDSA, or Elliptical Curve Digital Signature Algorithm. This algorithm is considered very strong with shorter key lengths and provides

reasonable signature verification speeds. It requires a minimum private key size of only 160 bits, producing a digital signature of 320 bits (40 bytes). The public key companion in this case is 161 bits (21 bytes).

These algorithms are proposed for use by ICAO for the Digital Signature authentication application discussed here, with ECDSA recommended and perhaps treated as a default. In addition, the *hashing algorithm* for calculating the digital signature is proposed as the Secure Hash Algorithm ***SHA-1*** 9so as to avoid the necessity of specifying which such algorithm was used in the digital signature.

The summary information regarding these algorithms is presented in the table below, along with the proposed "algorithm ID" code for the LDS specifications.The key lengths noted are considered acceptable by the security community at this time for secure usage in the medium to long term.

Algorithm	ECDSA	DSA	RSA
Proposed LDS Algorithm ID	01	02	03
Signing Key Length (bytes)	20 (160 bits)	20 (160 bits)	256 (2048 bits)
Relative Signing Speed	Fast	Medium	Slow
Signature Size (bytes)	40 (320 bits)	40 (320 bits)	128 (1024 bits)
Verification Key (bytes)	21 (161 bits)	128 (1024 bits)	136 (1088 bits)
Relative Verification Speed	Medium	Slow	Fast

Figure 7 Comparison of PKI Algorithms

The choice of PKI algorithm from the above can be made with regard to the medium chosen for the MRTD and the desirable speed of verification at the border. For present MRTDs with limited data storage space, ECDSA might be the best choice because of reduced Digital Signature and public key size.

For more advanced forms of MRTD with larger data space, RSA might be a better alternative due to its fast verification speeds at borders; this comes at a cost of slower original signing speeds, not potentially a difficulty with fast HSM's in the country secure signing sites, and longer public keys. There may be other alternatives that can be used as well, and the LDS can accommodate them. Each border system of each country, and the ICAO PKI certificate, will recognize multiple choices of algorithm.

5. CONCLUSION

The border security benefits of digital signatures is increasingly recognized by a great many countries and international organizations today, and is often seen as one of the cornerstone of changes to be made to border crossings and nationality security in this area, which developments also include biometrics, advanced card formats, and other features.

Biometrics and contactless chip technologies can be approved since the use of digital signatures will be necessary to protect the biometric and other digitized data on MRTDs, particularly on contactless chips.These initiatives go hand-in-hand, since implementation without Digital Signature protection represents a weaker and less secure arrangement

No form of MRTD is excluded from the benefits of this Digital Signature initiative; even present paper-based MRTDs can incorporate a Digital Signature for the MRZ, plus at least a highly compressed facial image of the MRTD photo for human inspection if not machine verification. And all special advanced card or future technologies with greater storage can be used for this program.

BIBLIOGRAPHY

[1]http://www.id.ee/link.php/1038
Tanggal akses: 17 Mei 2009 pukul 20:15

[2]http://www.isode.com/solutions/mrtd
Tanggal akses: 17 Mei 2009 pukul 20:25

[3]http://www.mcs-group.com.my/ePassport.htm
Tanggal akses: 17 Mei 2009 pukul 20:35

[4] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.