PKI Digital Signatures For Machine Readable Travel Documents

ICAO/TAG NTWG

TECHNICAL REPORT

Version 4

A Proposed Methodology for an ICAO PKI Infrastructure for Implementation of Digital Signatures on MRTDs.

April 19, 2003

Prepared by Passport Canada

Table of Contents

Document History

DATE	DOC	TITLE
21-Jun-2002	1	Encryption, PKI, and E-Commerce Standards and Applications for Machine Readable Travel Documents
6-Dec-2002	2	Addendum 1 – Simplified Implementation of Digital Signatures for Machine Readable Travel Documents
17-Mar-2003	3	Addendum 2 – A Methodology For Implementation of PKI Digital Signatures on Machine Readable Travel Documents
19-Apr-2003	4	PKI Digital Signatures for Machine Readable Travel Documents

PKI Digital Signatures for Machine Readable Travel Documents

1. Scope and Purpose

1.1. This Technical Report is intended to provide guidance and advice to States and to Suppliers regarding the application and usage of modern public key infrastructure (PKI) schemes for the implementation and use of Digital Signatures with Machine Readable Travel Documents ("MRTDs") complying with the specifications set out in ICAO Doc 9303 Part 1 (Passports), Part 2 (Visas), and Part 3 (Size 1 and Size 2 Official Travel Documents). This use of PKI technologies and Digital Signatures is primarily intended to augment security through automated and self-contained means of authentication of MRTDs and their legitimate holders. This Technical Report documents and recommends ways and means and specific methodologies to implement such international MRTD authentication through Digital Signatures.

2. Introduction

2.1 Technology, as well as terrorism, 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, countered by sophisticated physical security features advocated by ICAO to be used in the documents themselves[1], the impressive development of computer and print technologies that puts counterfeit and document tampering capabilities in the hands of many, makes it imperative that MRTD standards and recommended practices be bolstered on a continuing basis to detect and deter such new threats. This is an endeavour of constant vigilance and effort, particularly after September 11, 2001. The threat of other acts of international terrorism requires that security mechanisms be constantly refined and augmented in order to absolutely minimize the opportunity for an individual to cross any border with false credentials.

2.2 The use of new and advanced methods of protecting against false credentials is becoming an active program in many countries. For example, the United States has passed legislation[2] which advances specific requirements for incorporation of "biometric and document authentication identifiers" on MRTDs used to enter the USA, namely visas issued by its own foreign service offices and all passports and other MRTDs issued by countries "designated to participate in the (US) visa waiver program …as a condition for designation or continuation of that designation".

[1] ICAO Technical Report *Security Standards for Machine Readable Travel Documents*, 2001

[2] The US *Enhanced Border Security and Visa Entry Reform Act of 2002*

2.3 These biometric and document authentication requirements are to be computer-assisted, as the same legislation dictates that the US "shall install at all ports of entry of the United States equipment and software to allow biometric comparison and authentication" of all such US visas and foreign MRTDs. Moreover, these measures are to be implemented by October 26, 2004. Many States have similar interests and objectives in augmenting the security and authentication features of MRTDs for their own security purposes and to cooperate in international efforts to prevent terrorist activities.

2.4 ICAO standards are to be used in the implementation of the above legislation, as the same act specifies that such visas and MRTDs shall be "tamper-resistant and incorporate biometric and document identifying standards established by the International Civil Aviation Organization". As such, it is essential that ICAO move forward quickly in the finalization of its standards in these areas.

2.5 Since December 2001, ICAO and the TAG New Technologies Working Group (NTWG) has been evaluating the role that encryption technologies can play in document authentication and security. This has progressed through a number of stages to the point of developing today where a methodology and suggested costs can be proposed.

2.6 The TAG/NTWG has also been very active in the research in two additional areas, the incorporation of biometrics into MRTDs, which provides strong means of self-contained validation of the rightful bearer, and the growing use of high-volume advanced technologies in MRTDs, such as the use of contactless RF-based IC circuits ("contactless chips"), to permit biometric storage of larger biometric images and to further facilitate security. Both of these initiatives have been fast-tracked for the same reasons of augmented international identity and document security.

2.7 However, both the biometric initiative and the contactless chip initiative depend on the implementation of Digital Signatures on the same MRTDs. Unless data recorded, such as biometric and identity (MRZ) data on contactless chip media, can be self-authenticating through the use of PKI Digital Signatures, these initiatives are exposed to fraud and counterfeit. As a consequence, ICAO/TAG must consider this PKI initiative in an integrated fashion with others being reviewed.

2.8 This new Technical Report represents the culmination and consolidation of NTWG PKI work to date, and presents to ICAO/TAG a specific set of recommendations and methodologies to proceed with Digital Signature implementation in the ICAO MRTD community of States. In the following material an understanding of PKI cryptography and terminology is assumed. Readers seeking further clarification or information are referred to Annex "A" to this Technical Report for a tutorial on this subject, and to the Glossary and Reference sections.

3 Digital Signature Applications for ICAO MRTDs

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

3.1.1 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 DS 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.

3.1.2 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.

3.1.3 On a paper-based or inked MRTD the digitized MRZ data with the DS 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.

3.2 The DS 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 DS 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 DS will not match.

3.3 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 DS. 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 DS. 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 DS protecting the digitized data, photo substitution is not workable since the digitized (and DS-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.

3.4 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 computer-based 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.

3.5 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 DS 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.

3.6 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. In the following sections of this Technical Report a specific infrastructure and methodology will be described as a means of implementation of this program.

4 The Case for A Simplified PKI Infrastructure for ICAO MRTDs

4.1 The principles of digital signatures and of public/private key encryption schemes have evolved in their use to become highly complex in their application to modern scenarios. Their prime use is in Internet transactions, where keys must be trusted across a broad range of users and agencies; this has resulted in elaborate systems of key certificates, where public keys are issued as “certificates” which are digitally signed by trusted issuing organizations called Certificate Authorities (CA’s). The trust in these CA organizations must be further verified by higher-level CA’s in a trust hierarchy, each one in the hierarchy issuing the key and signed certificate for the one beneath it in the hierarchy. The top gun, so to speak, is the so-called “Root CA”. Different hierarchies must cross-certify each other to establish trust in the keys issued by each with the other, and the whole is a large and sophisticated infrastructure.

4.2 These hierarchies and practices are further described in Annex “A”. However suffice to say that in the commercial world there are serious difficulties with the complexities of such infrastructures. The need for cross-certification among different hierarchies is complicated by the trust that must be placed in each other’s security policies and practices, and public key access for individuals and corporate entities must be carried out, usually over the Internet, on a very frequent basis. A further complicating factor is the need for Certificate Revocation Lists

(CRL's), indicating where a key (certificate) holder no longer has the rights to that key for whatever reason. The need to verify certificates for each and every transaction often implies multiple accesses to CA records and to CRL records in different databases, a complex requirement.

4.3 The ICAO operating environment is different from the above commercial environments, and fortunately there has been work recently in looking at the whole area of the PKI infrastructures and simplifying implementation models for specific applications where special circumstances exist. For example, in a recent article in the IEEE Computer Magazine by Peter Gutmann of the University of Auckland[3], where many of these PKI infrastructure difficulties are detailed, he states:

> *In many situations, no PKI* (certificate infrastructure) *is necessary, vendor claims to the contrary. This holds particularly true when two or more parties have an established relationship. For example, the secure shell protocol avoids dependence on a PKI by having the user copy the required public keys to where they're needed, an approach feasible for its application domain.*

He goes on further to say, in reference to the difficulties of managing certificate revocations:

> *If possible, design the PKI so that it does not require certificate revocations. The best way to handle revocation is to avoid it entirely.*

4.4 These circumstances and objectives for simplification apply to the ICAO MRTD authentication requirement, where the number of users is small relative to the commercial world, where the users represent a closed group for a single application, where keys will be relatively few in number and remain relatively fixed, and where the application users represent as a peer group with all states that issue MRTDs cooperating for the mutual security and benefit of all.

4.5 Likewise, the question of public key revocation does not really apply (as it would for individual users), since the unlikely event of a compromise of any country private key used during some period to sign many MRTDs cannot deny that documents were indeed signed using that key. The Digital Signatures applied are meant to last for lengthy period and are not intended for every day transaction purposes. In the rare case of key compromise, a simple caution mechanism can be used to warn states to view those documents more closely.

4.6 As a consequence, the following sections present as a simple customized approach that will enable the MRTD community to fast-track implementation of this application and take advantage of its benefits without attempting to address larger PKI policy issues and complex hierarchies. A form of certificate is used for security purposes, along with a proposed methodology for public key (certificate) circulation to all member States, but the special infrastructure is customized and

[3] *PKI: It's Not Dead, Just Resting*, Peter Gutmann, IEEE Computer Magazine, August 2002.

simplified for ICAO/TAG purposes.

5 Overview – ICAO/TAG DS Infrastructure

5.1 The ICAO PKI application for DS implementation must operate in a completely peer-based user environment, with each country independent and autonomous in the matter of MRTDs and security, and yet motivated to cooperate with all others for mutual protection against wrongful admittance and counterfeit travel documentation. Unlike commercial applications, it is impossible to propose a solution where any central authority, or agency such as ICAO, can ever assign, maintain, manage, or even know the secure private keys of any nation; despite many strategic alliances among participants this will not be a trusted solution and will not be successful.

5.2 Nonetheless it is integral to the program to have an efficient and commonly accepted means of sharing and updating the set of public keys in effect for all non-expired MRTDs in existence for all participating countries at any time. Unlike the State autonomy necessary for the control of private keys, there is nothing controversial about the sharing of public key information necessary to make the scheme work.

5.3 With this in mind, the proposed custom implementation for ICAO MRTD digital signatures has been set out to consist of two main components, as follows:

5.3.1 **Secure In-Country Key Generation.** Each participating State will install its own secure facility to generate key sets for different periods of time, these will be used to compute the DS to be applied during that period to MRTDs issued. This system or facility will be well protected from any outside or unauthorized access through inherent design and hardware security facilities. Despite the independent and autonomous nature of these in-country systems, they will conform to ICAO specifications and recommendations just as is done today with 9303 standards for global cooperation and protection.

5.3.2 **ICAO Directory Services**. In order to efficiently share the corresponding public keys of all countries, it is proposed that ICAO develop and provide a Public Key Directory (PKD) Service to all participating States. This is a simple service, which will accept information on public keys from all countries, store them in a PKI directory, and notify and disseminate this new key information to all other countries. These countries will likely download these keys into their own border entry systems, or may simply use the ICAO directory service as a reference when required to determine the public key to use with a country's MRTD.

5.4 Each public key generated by each country (corresponding to a new MRTD signing key they intend to use) would necessarily be forwarded to ICAO, and therefore to the ICAO MRTD community, with significant additional public key information (validity dates, MRTD types, PKI algorithm used, user or issuing location, etc.) and itself be digitally signed as a secure communication by the issuing country. This package of data, including the public key, public key information, and the country's digital signature, forms a "public key certificate"[4].

5.5 Although the set of public keys in use by all States at any time would not be numerous there are still issues of practice for all members of the directory service; each time a country generates new keys all other countries must access the ICAO directory service and download the new information for storage and use by their internal border systems. Alternately a country could opt to check the public key with the ICAO PKD for each passport presented; however this is impractical in real life situations since keys are relatively static and so repeated directory access to obtain the same public key would often be superfluous. Nonetheless, even where public keys are downloaded into border control systems, occasional key confirmation requests would be made of the ICAO directory service in individual cases.

5.6 An alternate and potentially better way to distribute keys associated with specific MRTDs would be to include the public key as well as the DS on the MRTD itself. In this way signed MRTD data could be directly checked using the public key contained in the (secure) certificate, and the ICAO PKD service would only serve as a confirmation point as deemed necessary by each country. However it must be recognized that present MRTDs have little space to accommodate the resulting information load, at best a 2D bar code might be able to accommodate a compressed photo image with the digitized MRZ and the DS only. In this regard the ICAO directory service would be the main dissemination point for public key certificate information.

5.7 Increasingly, however, ICAO and its NTWG are envisaging MRTDs utilizing advanced technologies such as contactless chips and optical memory cards. These technologies have much more space for the inclusion of the DS and the full public key certificate data, as well as one or more larger biometric images and templates to be used for both human and automated verification of the bearer. In this eventuality, with the public key on the MRTD itself, the public key download requirement from the ICAO PKD will be lessened as long as sufficient trust was established in the validating certificate contained on the MRTD. The ICAO PKD would serve as a backup and confirmation point in this regard, but not necessarily as the central download point for all new country public keys in each instance of change. Nonetheless the role of the ICAO directory service is key to this infrastructure and application.

[4] The use of the term 'certificate" herein refers to the typical PKI mechanism whereby a public key is signed by a trusted certificate authority to validate it. However it is not implied here that all data incorporated into standard certificates need be included in the ICAO version, since the application environment is a closed loop and not intended for use widely and generally on the Internet, even though they will conform to the ISO X.509 Version 3 public key certificate format or other international PKI standard for certificates.

5.8 These approaches are discussed in detail in the next sections with specific methodologies proposed for implementation.

6. Proposed Methodology and Infrastructure

6.1. As discussed previously, in the proposed 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.

6.2. The proposed 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 1 below.

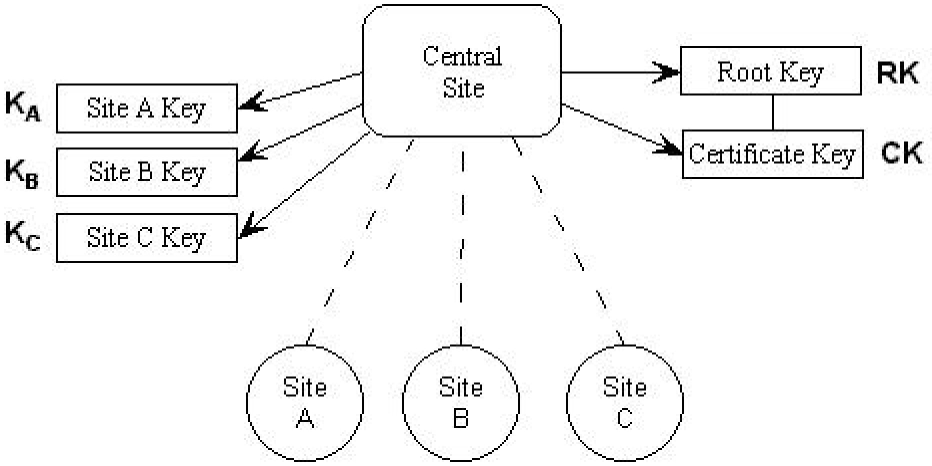

Figure 1 – Central Key Generation In Each Country

6.3. In Figure 1, a country with 3 issuing (printing) sites is assumed for purposes of explanation. In this case, a key pair (K_n) 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 proposed scheme.

6.4. The public key portion of each site-signing key (K_n) 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 DS value and returns the DS to the site for printing on the MRTD.

This is shown in Figure 2 below.

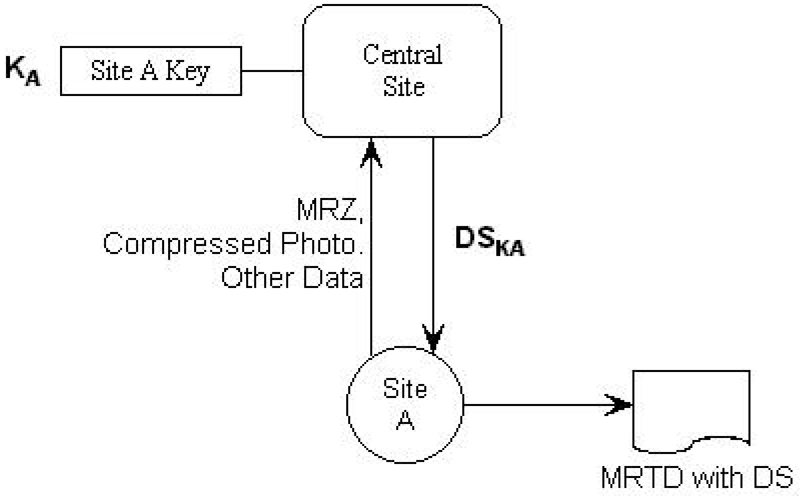

Figure 2 – Basic MRTD Signing

6.5. 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 DS. Proper electronic security measures need only be implemented in one location.

6.6. 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 so-called 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:

6.6.1. 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;

6.6.2. Key generation for multiple sites and multiple types (of MRTDs, for example), through partitioning;

6.6.3. 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;

6.6.4. Very secure entry/update restrictions, with such protection as multiple-person authorization for any update or change and robust individual identification standards. Many of these devices are validated to FIPS 140-1 Level 3[5] specification or equivalent.

6.7. The Secure Key Management System and general country configuration is shown schematically in Figure 3 below.

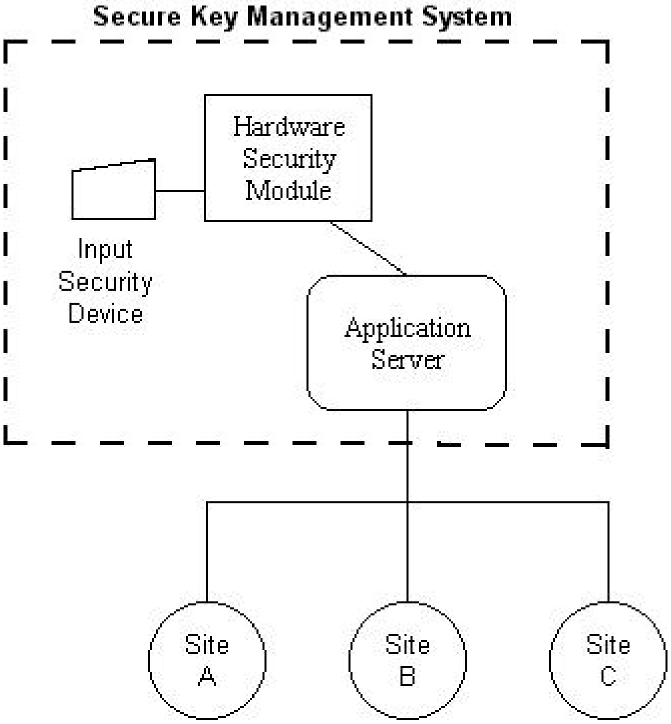

Figure 3 – Schematic of a Country Secure Key Management System

6.8. 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[6] 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.

[5] Federal Information Processing Standards (FIPS) Publication 140-1, *Security Requirements for Cryptographic Modules*.

[6] ISO/IEC 9594-8/ITU-T Recommendation X.509, *Information Technology – Open Systems Interconnection: The Directory Authentication Framework*, June 1997.

6.9. The proposed methodology for the ICAO directory update service and signing mechanism is shown in Figure 4.

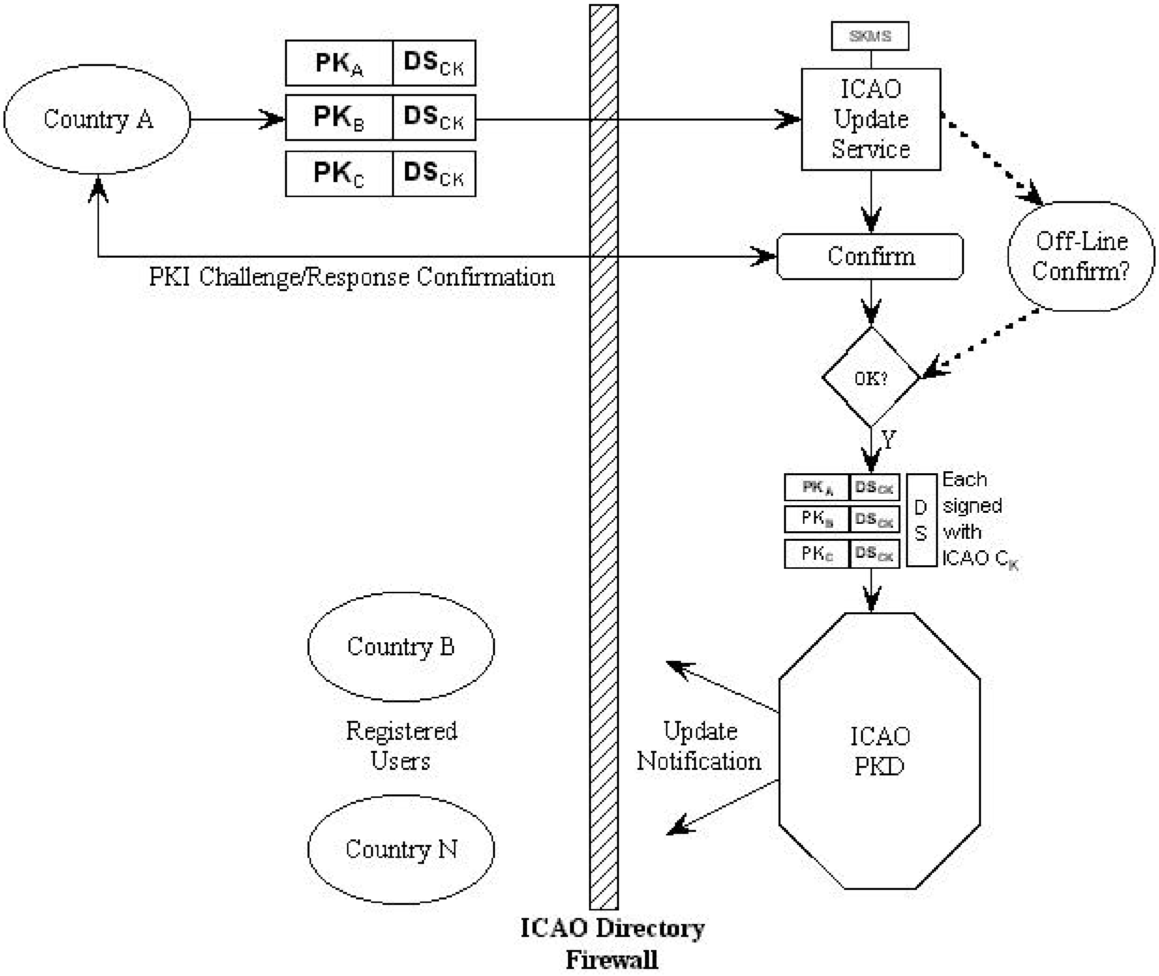

Figure 4 – Proposed ICAO Public Key Certificate and Update Process

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

6.10.1. Country A (in this example) has generated three key pairs for each of its 3 sites (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 1). This CK is very static and is known to all other ICAO member countries through a similar update mechanism upon enrollment in the MRTD DS 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.

6.10.2. 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:

6.10.2.1. 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.

6.10.2.2. 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 DS 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.

6.10.3. 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.

6.11. 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:

6.11.1. 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;

6.11.2. 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.)

6.12. 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.

6.13. 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.

6.14. 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.

6.15. The DS process applying to advanced forms of MRTDs is shown in Figure 5.

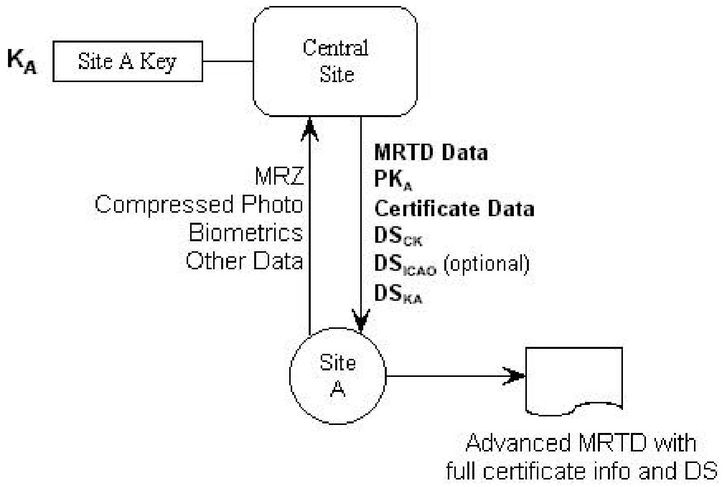

Figure 5 – Future Signing of Advanced Forms of MRTDs

6.16. As can be seen from this diagram, the signing of these MRTDs proceeds in the same way as previously, where the central SKMS site generates and protects all issuing site keys and carries out all of the DS and cryptographic calculations. However in this case it also returns the ICAO key certificate information as well as the DS to the issuing site to incorporate on the MRTD. This certificate format and content is exactly the same as is forwarded to ICAO for the PKD, and so this arrangement is fully compatible to what is being proposed for present forms of MRTDs. Equally importantly, no significant changes to any country's border system need be made if they have previously accommodated the ICAO directory service source of downloadable certificates; the certificate available on the ICAO directory service is the same as that now appearing on the MRTD document itself.

6.17. In the diagram additional information is suggested for inclusion in the signing operation. Such things as a more detailed (less compressed) facial image (sufficient not only for human inspection but also for facial recognition algorithms), along with other biometrics, may be included at the discretion of the country and in accordance with evolving international practice. The Logical Data Structure (LDS) developed by ICAO/TAG accommodates a variety of such information. The DS computed by the country's central site and returned for MRTD issuance to the issuing office will incorporate all of these data fields plus the full set of certificate information. (Note that the additional signing of the certificate with the ICAO signing key, obtained from the ICAO directory notification and update process, should also be included to form a full ICAO PKI certificate in the same form as appears in the ICAO directory)

6.18. **Concluding Remarks on the Proposed Methodology.** Use of the methodology and infrastructure described in this section provides a very simple and effective approach to ICAO and its MRTD standardization responsibilities. Firstly, because the application is designed for the specific MRTD signing purpose, with a closed community of states as users, the number of signing keys in existence at any time is not large (compared to open international financial utilization, for example) nor subject to frequent change. Secondly, again because of the private closed nature of the application, much of the complexity of a "standard" PKI infrastructure can be avoided; for example, formal CRL's (Certificate Revocation Lists are unnecessary and the structure of ICAO certificate keys might be simplified, without the intricate "cross-certification" and multi-organizational certificate hierarchies of more traditional PKI implementations. Thirdly, the simple infrastructures proposed can be implemented in relatively short time frames and at very reasonable costs, enabling the benefits of the program to be realized sooner rather than later for increased global security. Finally, the private closed nature of the application will hopefully permit the application to be implemented in each country without ponderous and lengthy entanglements in each country's large-scale PKI policies and practices, which may then take longer and cost dramatically more. It is hoped in this regard that the application will be judged in each country as an exception, with a closed and limited utilization, and one which has significant urgency associated with it given present world situations and the need for greater ID and biometric security.

7. Using The LDS - Logical Data Structure

7.1. Considerable work has gone into the Logical Data Structure ("LDS") specifications for digital recording of MRTD data on to various forms of 9303 standard MRTDs. Recent updates have been issued for Sequential File Formats (such as printed MRTDs)[7], particularly **9303 Part 1 Passports** and **9303 Part 2 MRTD Visas,** as well as for Integrated Circuit Cards (smart cards)[8] for **9303 Part 3 ICC** technologies. Other LDS specifications apply to Optical Memory Cards, **9303 Part 3 OMC** technologies**.**

7.2. The LDS specifications developed for Part 3 MRTDs are of a type used for modern data base implementation specifications, using extensive tags and descriptors for each data element and type, for specific read access as required. Only the data required need be read from these devices. The sequential specification applies to MRTDs where the data appears and must be read all at one time, on a printed MRTD with a 2D bar code, for example. The data area is therefore classified as a "Binary Large OBject" or "BLOB" in the LDS, and the data elements included in it are presented and described with simpler styles.

7.3 Details of how the LDS applies to the proposed PKI infrastructure, with specific examples, are contained in Annex "B' to this Technical Report. The LDS is an on-going development effort within ICAO/TAG, and the full specification for the LDS for all forms of MRTDs will be reviewed and possibly updated to accommodate the proposed implementation of Digital Signatures. Nonetheless the proposed DS application is compatible with the LDS.

8 PKI Algorithms.

8.1 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

8.1.1 **DSA**, or Digital Signature Algorithm, as specified in the US *Federal Information Processing Standard (FIPS) 186-2, Digital Signature Standard (DSS)*. 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..

[7] *Version 0.5 MRTD Logical record Format Mapping – Sequential File Format*, 11 April 2002

[8] *Mapping of Logical Data Structures to integrated circuit(s) cards (ICC) Ver0.1*, 8 April 2002

8.1.2 **RSA**, or Rivest Shamir Adleman algorithm, as specified in PKCS #1, v2.0 *Public-Key Cryptography Standard # 1 – RSA Cryptography Standard*. 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..

8.1.3 **ECC/ECDSA,** or Elliptical Curve Digital Signature Algorithm, as specified in ANSI X9.62 *Public Key Cryptography for the Financial Services Industry: ECDSA*. 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).

8.2 These algorithms are proposed for use by ICAO for the DS 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*** [9]so as to avoid the necessity of specifying which such algorithm was used in the digital signature.

8.3 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

Table 2. Comparison of PKI Algorithms

[9] FIPS 180-1 Federal Information Processing Standard 180-1, *Secure Hash Standard*, US Dept. of Commerce, National Bureau of Standards, 1995

8.4 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 DS 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.

9. Estimated Costs and Financing

9.1. Part of this work involved the practical consideration of costs and possible financing alternatives for implementation of the ICAO DS application. Of course, despite the details of potential configurations and implementation strategies discussed with industry for this purpose, it is not possible at this level to be definitive on this matter. Nonetheless the simplicity of the infrastructure proposed, which was developed with the aid of many industry discussions, did permit representative scale-of-magnitude estimates to be determined.

9.2. This section presents this information with the following caveats:

9.2.1. Such estimates are representative only and are not guaranteed to be realizable in actual RFP or competitive tender situations, even though knowledgeable industry representatives have provided and reviewed them.

9.2.2. The costs estimates are strictly for direct costs: namely hardware, software, technical integration, and third-party management fees pertaining to the PKI operation only. Specifically excluded are any other related or secondary costs, such as those associated with internal country communications between issuing sites and the central secure signing site of the country, costs to design, test, and implement DS printing on existing or future MRTDs of a country, or any in-country costs for contract management and project supervision for the implementation effort.

9.3. In developing these costs, a typical set of hardware components was selected for functionality and pricing. In addition it was assumed that the ICAO application development would take advantage of such evolving tools as XKMS (XML Key Management Specification), now offered by several organizations to greatly simplify the coding and implementation of cryptographic operations.

9.4. Costs are broken down into the following components:

9.4.1. Initial development costs, including overall design, specification, and documentation of the PKI infrastructure, plus development and integration of the ICAO PKI Directory Service and development of a pro-forma country secure key management and signing site. These development projects are to result in a pro-forma working infrastructure for the ICAO program, for demonstration and licensing to other participating countries;

9.4.2. Consulting and contract management fees for the initialization program, incorporating planning, RFP's, contracting and contract management, and country/committee liaison for the program on behalf of ICAO;

9.4.3. Country implementation estimates (hardware and ICAO PKI implementation only);

9.4.4. Actual ICAO PKD integration and start-up as an operating directory service;

9.4.5. Annual high-level maintenance and support contracts for typical country installations (this will vary from country to country and may be accommodated by existing internal resources);

9.4.6. Annual estimated costs for third-party outsourced full operation and management of the ICAO PKD on behalf of ICAO.

9.5. The initialization effort, to design and specify fully the ICAO MRTD signing infrastructure, plus the development and implementation of a pro forma country site as well as the PKD, is important both to evidence proof of concept but also to test functionality and performance of typical operations. It is also essential to provide a working example to all countries of a sample realization of the ICAO infrastructure, which they can easily access by direct licensing or match through equivalent, and equally secure, implementations in their own jurisdictions. The existence of a test site, combining both the ICAO Directory and a typical or pro-forma secure country site will prove invaluable in infrastructure maintenance and support as well as on-going development and testing.

9.6. The cost estimates for the above categories are detailed in Annex A to this Addendum, and are summarized as follows ($US):

Total Initialization and One-Time Costs	***$800,000***
Total 3rd Party ICAO PKD Operating Costs/Yr	***$400,000***
Country One-Time Costs	***$150,000***
Country Annual Maintenance and Support/Yr	***$ 50,000***

9.7. These costs are based on industry input and are again restricted to specific costs of the new and installed ICAO PKI infrastructure components. Other costs for

MRTD print alterations, governmental management, overheads, and all other related costs are not part of these estimates.

9.8. The above cost estimates are an indication of the simplified structure and operating profile of the proposed ICAO implementation. What it also means, however, that for direct costs to get involved with this program, ICAO and its member community of states must finance some $800,000 - 1,000,000 $US of expenditures. Presently there may be no budgets or available means to raise this money within ICAO or its member states. However the program offers many benefits, so the following deals with a possible financing scenario.

9.9. **Financing.** This program should obviously be eventually self-financing, through contributions from the member states deriving the benefits from its availability. As is typically the case with government budgets and expenditures, however, capital financing, even with leases, may be restrictive, and the amounts needed are often large enough to require serious approval cycles. This may not be the case, however, with licensing fees and other operating expenditures, particularly with regard to participation in desired international programs such as this one.

9.10. Accordingly, a financing mechanism is suggested which may be feasible for most states, consisting of the following components:

9.10.1. Through whatever international resources are available to it, such as sponsorship (loan, grant) by one or a few states or commercial financing guaranteed by a state, ICAO needs to avail itself of sufficient funds to undertake the first steps of the program. This will amount to at least $800,000 for the direct costs estimated in Annex A, plus additional funds as required for other added costs (administration, travel, internal coordination).

9.10.2. The results of the first stage will include complete infrastructure specifications and documentation plus a working and proven test bed for both the ICAO PKI Directory and a typical country secure key management and signing site site. These will form the basis for adoption and implementation by many states.

9.10.3. After development and test/acceptance of the above by ICAO, and presumably with several states giving it support and a commitment to incorporate the DS in their MRTDs, ICAO would then formally adopt the program, install a working Directory Service (proposed to be set up and managed by a third-party professional IT group), and implement the specifications and documentation as new ICAO standards. These standards would presumably be a special part of 9303 and relate to other such standards as biometrics and the LDS.

9.10.4. Participating countries would commence to design and install their own internal infrastructures, which will often simply involve purchasing and adapting the ICAO pro-forma in-country site to their own requirements and configurations. It is proposed for financing the entire initiative that each such participating country pay an initiation or sign-up fee to ICAO, plus an annual fee for continued membership in the PKD and ICAO PKI initiative, which could again be cast as a license renewal fee.

9.10.5. These fees would both reimburse ICAO for its initial investment and also pay for on-going 3rd-party management of its PKD as well as administrative costs associated with the continuing program. In order to assess order of magnitude minimums for such fees, based again only on the direct costs estimates included in this report, the following analysis was prepared to allocate costs over 5, 10, 15, and 20 participating States.

Table 3 – Estimated Fees Per Country to Finance the ICAO PKI DS Initiative

ITEM	5 STATES	10 STATES	15 STATES	20 STATES
Country Sign-Up Fees	$160,000	$80,000	$53,000	$40,000
Annual Participation Fees	$80,000	$40,000	$27,000	$20,000
Total Country Set-Up Costs Est.	$310,000	$230,000	$203,000	$190,000
Total Country Annual Costs Est.	$130,000	$90,000	$77,000	$70,000

9.11 Clearly the participation of even a small number of states in the program, say 10-20, makes the financing of the direct costs of the program very inexpensive and realistic. (Equally clearly, if at least 10-20 states do not agree to proceed at the outset, the program may not go forward!) The net costs per country, including initiation fees and annual membership fees as well as configuration and implementation of its in-country site, are also not onerous for any state; even with the addition of other costs such as the design changes necessary for their MRTDs, the program represents a very realistic opportunity to implement such a scheme in the world through ICAO standards and NTWG work, for the mutual security benefits of all states.

10 Conclusions and Next Steps

10.1 This document is one of a series produced as Technical Report initiative for ICAO/TAG, through the sponsorship of the NTWG, and at this stage has presented a viable methodology and infrastructure for ICAO to guide and standardize the implementation of PKI digital certificates on 9303-spec MRTDs around in the world.

10.2 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.

10.3 Few if any of these international initiatives, however, have proposed other than the conceptual incorporation of digital signatures on MRTDs or other ID documents, and often these efforts simply imply that a “standard” commercial-like PKI implementation of such schemes will eventually be adopted.

10.4 ICAO has, however, moved well beyond this stage, and has progressed to this point where a much simplified and specific, private-membership scheme is now being proposed that offers the advantages of greater simplicity than standard PKI infrastructures, with the attendant benefits of relatively inexpensive and relatively fast implementations. The approach meets the approval of encryption industry specialists, and represents a positive way for ICAO to exercise clear leadership in proposing not only the “what” but the “how” in this field. Through this initiative other ICAO work, such as 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 DS protection represents a weaker and less secure arrangement (for example, unsigned biometrics data could conceivably be forged, and signed RF chip documents without bearer biometrics could conceivably be skimmed or copied).

10.5 This ICAO initiative and proposed methodology is also technology-neutral, with the exception that MRTDs with larger data memory capacities will facilitate better biometric measurements and machine verification of biometrics (in addition to human inspection), and the inclusion of the ICAO-format public key certificate on the MRTD itself will facilitate more efficient border validation operations. However, no form of MRTD is excluded from the benefits of this DS initiative; even present paper-based MRTDs can incorporate a DS 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 via the LDS; none will provide any special benefits for this application other than costs of the memory required and the speed of data access.

10.6 Accordingly it is recommended that ICAO/TAG proceed with this PKI initiative on a fast track, along with its other NTWG efforts. Its leadership in the initiative will provide the world community with a very positive direction, and very likely facilitate widespread acceptance and improved border security in much shorter time frames that otherwise can been achieved.

10.7 The direction recommended for ICAO is described in the previous section on estimated costs and financing, inferring that ICAO provide up-front work on specifying and documenting the proposed infrastructure and develop a pro-forma country Secure Key Management System site and an pro-forma ICAO Public Key Directory service, both for testing and demonstration to the world community. To prepare for this stage, it is proposed that the immediate next steps be as follows:

10.7.1 Obtain TAG approval to proceed and direct an overall liaison effort through NTWG to proceed.

10.7.2 Initiate a detailed planning cycle which incorporates such elements as initial financing, project planning and scheduling, developing detailed statements of work and RFI/RFP activities, setting of program objectives and targets, liaising with other agencies and international bodies, and preparing communiqués for publication as deemed appropriate.

10.7.3 Provide a report on all aspects of the above plus a detailed plan and budget proposal to ICAO/TAG for approval.

10.7.4 Based on the results of that effort, and the approval of ICAO/TAG, proceed in accordance with the plan.

Glossary

ASN.1 – Abstract Syntax Notation 1: A notation commonly used to specify the syntax of computer data elements in communications protocols, including the X.509 public key certificate standard.

BLOB – Binary Large Object: A set of data elements defined in the Logical Data Structure (LDS) specifications which are recorded onto (MRTD) media, and read from the same media all at the same time, without benefit of tag descriptors specifying individual data element presence, length, and other attributes.

Certificate: A set of data provided in a standardized format (such as X.509) that reliably validates a public key and its rightful owner. The certificate contains the public key and related information, and a Digital Signature to authenticate the certificate's contents.

CK – Certificate Signing Key: A term used in this document to describe the private signing key used by each country to apply a digital signature to its ICAO-format certificates. These certificates describe and authenticate new keys to be used by the country to digitally sign its MRTDs; the ICAO-format certificates are forwarded to ICAO for inclusion in its public key directory for all countries to access.

DS – Digital Signature: An encrypted value for a set of data that results from mathematical computations on the data, using standard algorithms, to produce a unique if meaningless result called the hash result or digest of the data, followed by the encryption of this result to form a Digital Signature for the data.

DSA – Digital Signature Algorithm: an algorithm developed by the US Government primarily for use in computing digital signatures.

ECDSA – Elliptical Curve Digital Signature Algorithm: a special form of public key algorithm that provides strong solutions for digital signatures with shorter key lengths. It might be very appropriate for use for MRTDs with small available storage space for digital signatures.

HSM – Hardware Security Module: A robust and highly secure server device which is used to provide very high levels of protection for private keys and to efficiently and rapidly carry out encryption functions such as computing digital signatures, without release of the private key value.

PKD – Public Key Directory: A term used in this document to denote the ICAO Public Key Directory proposed for use by all countries to store and access all public keys used by countries to digitally sign their MRTDs.

SHA-1 – Secure Hash Algorithm #1: A data hashing algorithm standard commonly used to produce a hash result, or digest, for a set of data, which is then encrypted using the private key of the data originator to produce the Digital Signature of the data. See DS.

SKMS – Secure Key Management System: A term used in this document to describe the secure installation within each country, to generate and protect private keys used by the country to sign their MRTDs, and to compute these Digital Signatures using these private keys for all issuing locations in the country. Normally, HSM's would be used as part of these secure computer installation sites.

XKMS – XML Key Management Specification: A set of program development tools in XML now offered by several companies. They provide the ready means to quickly implement custom PKI solutions without the need for developers to code sophisticated encryption, digital signatures, decryption, and other typical PKI tasks.

XML – Extensible Mark-up Language: A modern language used in computer and communications applications to describe the nature and properties of information, so as to permit interchange of that information between computer systems without necessary advance knowledge by all recipient applications of the nature of that information. It is a significant improvement on HTML, which only describes how data should be formatted on the screen of a receiving user, and not what the information is.

References

ISO/IEC 9594-8/ITU-T Recommendation X.509, *Information Technology – Open Systems Interconnection: The Directory Authentication Framework*, June 1997.

Federal Information Processing Standards (FIPS), Publication 140-1, *Security Requirements for Cryptographic Modules*.

Federal Information Processing Standard (FIPS) 180-1, *Secure Hash Standard*, US Dept. of Commerce, National Bureau of Standards, 1995

Gutmann, Peter, *PKI: It's Not Dead, Just Resting*, IEEE Computer Magazine, August 2002.

Smith, Richard E., *Authentication From Passwords to Public Keys*, Addison-Wesley, 2002.

Adams, Carlisle, and Lloyd, Steve, *Understanding Public Key Infrastructure: Concepts, Standards, and Deployment Considerations*, New Riders Publishing, 1999.

Austin, Tom, *PKI – A Wiley Tech Brief*, John Wiley & Sons, Inc., 2001

Annex "A"

A Tutorial on PKI Technologies for ICAO Applications

I. Encryption and Decryption.

I.1 In order to understand how modern encryption technologies can be used effectively by the ICAO community, some basics must be understood, which is the purpose of this section.

I.2 *Encryption* and *decryption* are the fundamental components of the science of cryptography. Essentially, whatever the technique used, a private message is hidden, typically using mathematical algorithms and codes to transform the message into seemingly meaningless data. The coding and decoding of such information is carried out with a *key*, namely a string of data that is used with the algorithm employed to transform the original message to the coded string, or to decode the string to the original message text. Such techniques, and other means of hiding messages, have been in use for many centuries, of course with varying results and continuously upgraded sophistication. The ability to decode enemy messages, unbeknownst to them, has formed the basis for many significant military victories in history.

I.3 In traditional situations the same key is used to encrypt as well as to decrypt the information, and the length of the key and algorithm used, aided by the processing capability of computers, determine how effective the encryption is. This process, called ***symmetric encryption*** (because the coding and decoding keys are the same) is inevitably intended for and used by individual governments and private groups for protection of their confidential information and messages. For example, diplomatic messaging between a State and its foreign missions has used these techniques for a long time. Figure A-1 shows this schematically.

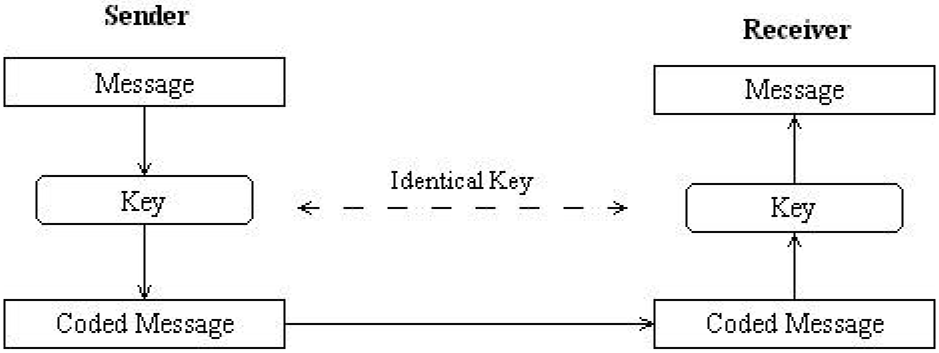

Figure A-1. Traditional Symmetric Encryption

I.4 The key used for coding and decoding of each must be of sufficient length and the algorithm used sufficiently robust that an acceptable level of confidence is achieved. Even so, a key may only be used once, a session key, or for a limited time such as a on single day.

I.5 One standard or "commercial-level" technique is called "Triple-DES", where DES is the Data Encryption Standard invented in 1975. This technique involves the use of three symmetrical keys and a triple coding process; the keys themselves are usually 64 bits in length (8 bytes) and this is generally regarded as representing agreeable protection for most commercial or limited-sensitivity government information protection. Higher levels and much more robust techniques are used for more sensitive information.

I.6 Traditional symmetric encryption techniques are not readily applicable to the ICAO objectives for MRTD data and MRTD document authentication, since they have to do with messaging and data protection of a private sort. The very fact of key sharing, where the keys used each time must be stored and available in more than one location, combined with the stringent secrecy required for such keys to prevent leaking of critical information, are not well suited to applications where documentation authentication and international interoperability is concerned. In the NTWG Policy Paper titled "Securing Data in Optional Capacity Data Storage Technologies", it was noted that encrypted data is data to be shared with a few trusted parties only (who would know or be able to retrieve the keys), and would normally be used to protect the privacy of personal data not directly associated with identity confirmation. The main reasons for this are:

I.6.1 Data used with MRTDs is open data, printed on the MRTD. Even the photo, a biometric image, is public. Encryption of this information using symmetric keys does not provide any further benefit of the sort associated with secret exchange of information as there is no essential privacy or security surrounding the information; and

I.6.2 The use of symmetric encryption requires sharing of secret keys and widespread distribution of these keys to States, which is impractical. This is made even more so since the keys themselves must be changed frequently in such scenarios to avoid the risk associated with any compromise of the codes used as keys.

I.7 There are nonetheless many applications that will involve MRTDs, particularly 9303 Part 3 card-based forms that may contain a computer chip, optical memory zones, RF contactless chips and circuits, 2D barcodes, or other advanced data storage and access technologies. These include facilitated border crossing systems, e-visa data for the private use of the visa-issuing country, or e-commerce, involving data above and beyond the basic MRTD data. This information will be securely encrypted and private, shared (by sharing the key) only among those States and commercial organizations that are partners in the application. However even in these cases the limitations and dangers of symmetrical encryption with the need for sharing of the single key used for each encryption stage, limits its practical usage because of the dangers of compromise involved. A much more robust encryption technology, generally known as ***asymmetric encryption***, lends itself much better to the overall requirements of ICAO and is described below.

II Encryption With Public Key Cryptography.

II.1 In the last twenty-five years completely new cryptographic methodologies have been developed which have revolutionized the communications industry, particularly regarding the Internet, and have enabled modern secure e-commerce and other activities to take place despite the openness of communications media. These techniques, known as Public Key Cryptography, and where the infrastructures associated with them called "Public Key Infrastructures" or "PKI", involve mathematical algorithms for encryption and decryption of information by separate but mathematically related keys in a key pair. Encryption carried out by one key of the pair must be decrypted by the other key, and vice-versa, so in this sense the operations are asymmetric. This is shown in Figure A-2 below.

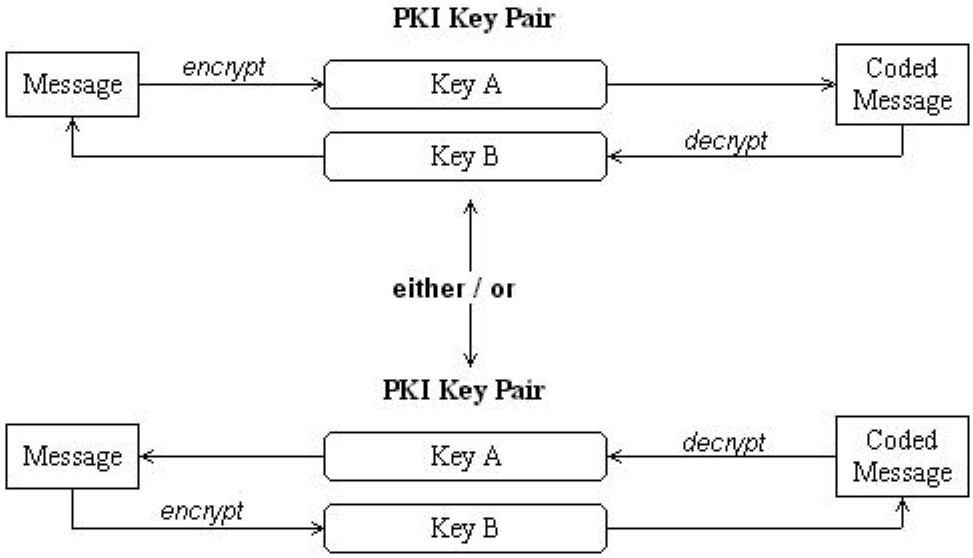

Figure A-2: Operation of Asymmetric PKI Encryption/Decryption

II.2 The significance of this new technology was that either key in the key pair may be used to encrypt, and this key cannot then be used to decrypt the encrypted result, only the other in the pair. Furthermore, *knowledge of one of the keys in the pair does not give any clues or easy path to knowing the value of the other key in the pair.* In fact, extremely extensive and effectively impractical (with adequate key lengths) brute force computational effort would be required to determine the companion key in a pair.

II.3 These unique strengths of PKI have been essential to many modern aspects of encryption and security today. Of particular significance compared to symmetric same-key techniques is the practice of designating one member of the key pair (assigned to an individual or organization) as a Public Key (hence the name Public Key Cryptography), and indeed made public, with the other member of the key pair declared the Private Key and kept secret. This ability takes away the weaknesses associated with key distribution in traditional circumstances, where the coding/decoding key must be communicated to and shared by several sources, and facilitates a number of special operations as described below.

II.4 **Secure Messaging.** Simple secure messaging between two parties can be carried out without revealing or sharing private keys with anyone. As shown in Figure A-3, the *sender* can encrypt the message with the *public key of the receiver.* This encryption key is not a secret, need not be protected, and cannot be used by anyone to decipher the message since the private key is not known nor distributed. Only the proper recipient of the message can decode the message, using the private key kept securely hidden.

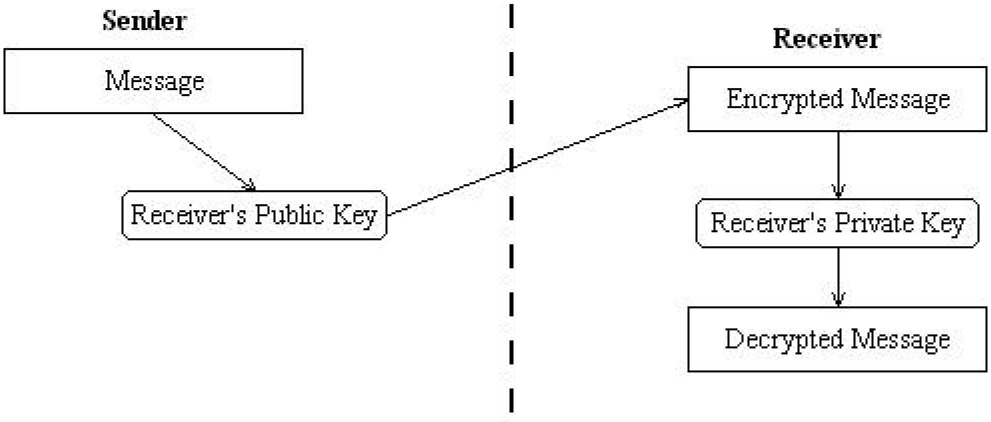

Figure A-3. Secure Messaging with PKI.

II.5 The above scenario is understandably critical for Internet exchanges and e-commerce where security of data (credit card numbers, for example) must be provided. In fact, sophisticated variations of the above scheme are used many times daily, often unbeknownst to the Internet user.

II.6 **Digital Signatures, Data Integrity, and Authentication.** Another important aspect of modern Internet usage, and of great significance to the ICAO community as well (as will be seen), is the ability for the sender to electronically sign all messages sent, even if these messages are not themselves encrypted. This feature is extremely significant, as means had to be found to replace the (albeit marginal) security of a handwritten signature on documents and contracts, especially in the electronic age of e-commerce and open communication of important messages. Like written signatures, they are necessary to give confidence and contractual weight to the information sent; it certifies that the supposed sender is in fact the actual sender, and that the recipient can take comfort in that knowledge. In addition, the sender cannot later repudiate the message by saying it was a fake or forgery. But what actually is a "digital signature" and how does it provide for data integrity?

II.7 Proof of source and non-repudiation using digital signatures are extremely important features of PKI, and its implementation using hashing schemes as described below, to compose an actual "digital signature", also provides the recipient with the comfort that *the data or information received has not been altered in any way*. In this way data integrity is assured or *authenticated*, despite the opportunity of tampering in open communications networks. This capability will also permit ICAO and its member states to authenticate MRTD data.

II.8 Digital signatures with all of these capabilities are implemented using *hashing techniques* on the information or message to be sent and signed. Specific and standard mathematical operations without any particular significance in and of themselves are carried out on the bits of the data message, resulting in a number or bit string called a *message digest* (or simply *digest*) that can only be formed with the algorithm selected and the data used in the hash process. This number is not an encryption, but just an arbitrary mathematical result that is a very sophisticated cousin of the check-digit calculations now carried out under ICAO 9303 specifications for MRZ fields.

II.9 Once the digest of the information is calculated, the sender uses his or her *Private Key* to encrypt the message. Again this key is not known or shared with anyone, so it can be considered a very secure key. The recipient, or anyone for that matter, can readily decode the digital signature of a message using the Public Key of the sender, by definition an open key, and use that key to verify or authenticate the content of the message; this is done by repeating the hash calculation on the message data itself, and comparing the results to the original hash digest. This process is illustrated in Figure A-4.

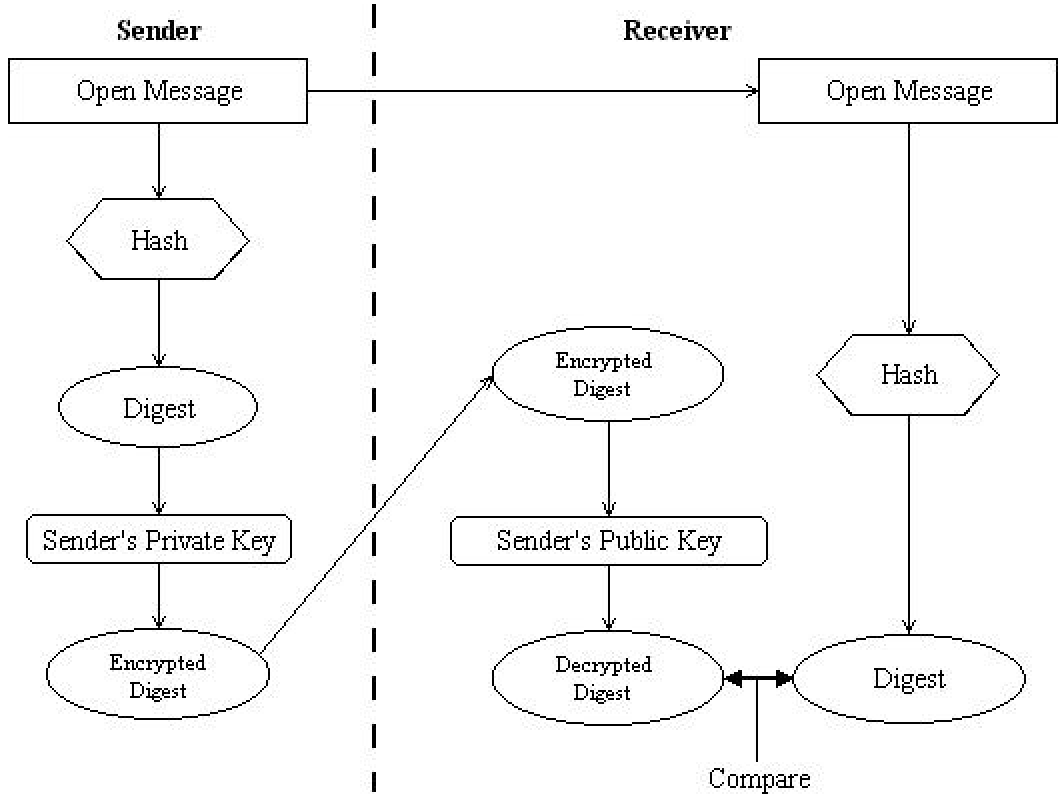

Figure A-4. Use of a Digital Signature to Authenticate an Open Message

II.10 It is important to note that *the two message digests must match exactly or the receiver will know someone has tampered with the message content*. This is critical: anyone attempting to change any of the content of the message cannot do so while preserving the integrity of the corresponding signature, since the Private Key used to generate the signature is not known to anyone other than the original sender. This demonstrates the strength of digital signatures, for authenticating the message as to source, providing for non-repudiation by the source, and ensuring that no element of the message has been tampered with in any way.

II.11 The true power of PKI technology can be realized where the message is encrypted and a digital signature is applied. This is shown in Figure A-5. The advantages to Internet traffic and to e-commerce are obvious and are made possible because of the nature of asymmetric key usage in PKI methodologies.

II.12 Encryption of the information or message with the recipient's public key as shown in Figure A-5 is distinct from the use of digital signatures in that it is only useful for private message sharing by one or a few entities. For example, a State might use it to register someone in a specialty program such as a border facilitation scheme and store the encrypted data on a card token, or use the technique to store and access its own visa information electronically. In all cases the information encrypted must be decrypted using a secret private key, whereas a digital signature provides protection against data tampering and certifies the source. The private key required would be known only to the entity itself, such as a state's immigration authority. If the information was to be shared by several states but nonetheless still protected by encryption (such as in a border facilitation program involving by several states), the data would have to be encrypted several times using the public keys of each of the states that need to read the data. Nonetheless there is still no need to share a sensitive symmetric key in these circumstances.

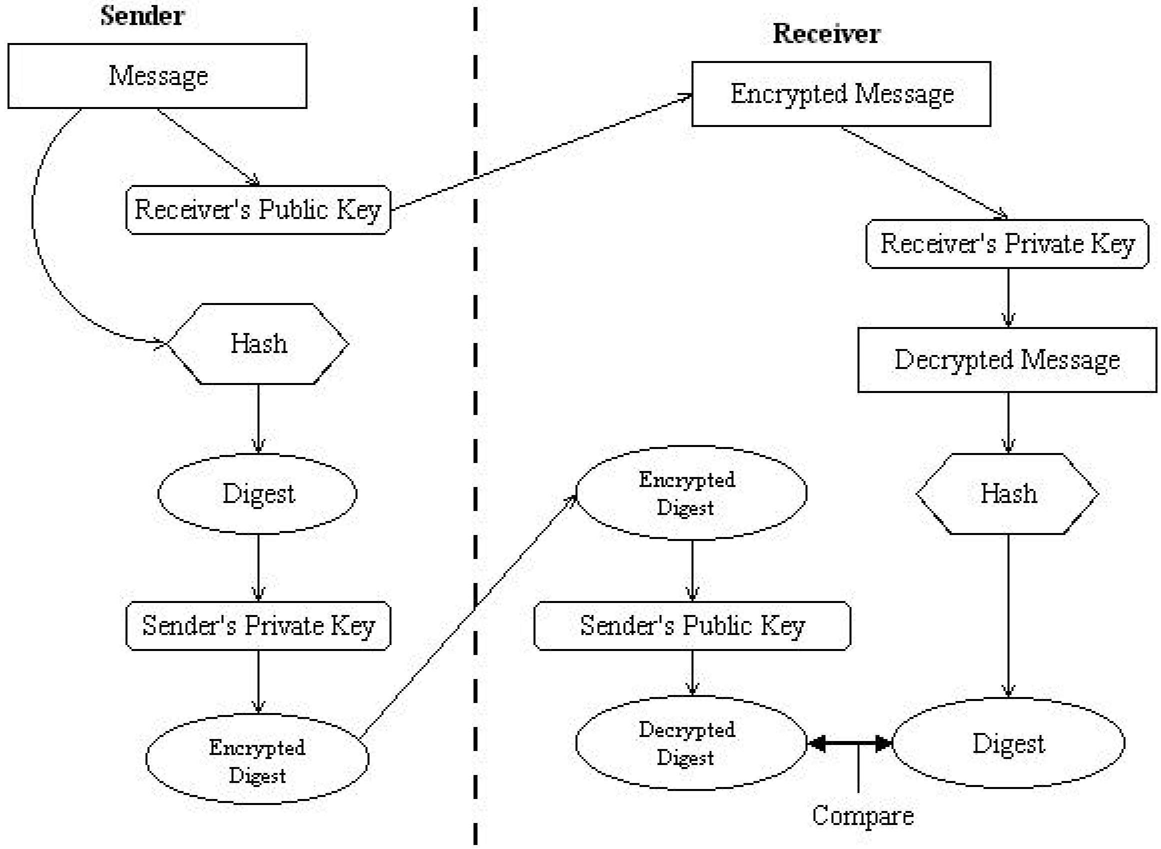

Figure A-5. Use of PKI Digital Signatures with PKI Encrypted Message

II.13 **Hybrid Protocols.** In some applications the combined use of symmetric key and asymmetric key protocols can be used to provide data protection. For example, the information and the digital signature, the latter being the message digest encrypted with the senders private key, can all be encrypted using a one-time symmetric key. That symmetric key can then be encrypted with the recipient's public key and sent along with the information and signature. In this case the recipient decodes the symmetric key with his or her private key, then uses the unscrambled key to decode the message and signature. Finally, the recipient uses the sender's public key to verify the digital signature and the data, by repeating the hashing process on the data. There are variants on this scheme, but notably the symmetric key can a) change for each usage, and b) not have to be secretly shared between sender and recipient prior to transmission. Of course the scheme relies on the security of the recipient's private key.

III PKI Key Issuance and Management

III.1 The benefits of PKI are numerous and very significant to modern e-commerce and Internet communications, and for the needs of ICAO as well. However there are significant security issues associated with its utilization, because of the ability with modern technologies to intercept messages, send message as an imposter, and indeed illegally enter private computers to steal data, including private keys. Many kinds of attack are feasible; if a client is trying to establish communications with a bank, for example, and the bank requests her public key, an interloper can intercept the messages in both direction and substitute his or her own public key and thereafter access the client's account.

III.2 Clearly, therefore, one of the basic assumptions of a PKI protocol is that keys used are properly issued and are to be trusted, that private keys are kept very secure, and that the systems using them to encrypt and/or sign documents are not accessible to the wrong parties. It was not enough to assume that individuals or organizations could simply announce that they are using a certain key pair and publish their public key. Rather, these keys must be issued and managed by trusted third-party organizations, to ensure that the identity of an individual or entity applying for a key pair has been checked and verified, that all others can rely on the public key subsequently issued, that the issuing entity is properly certified and authorized for such issuance, and that the keys used and are still valid, verifiable and secure in all aspects. It is interesting, and valuable for possible future ICAO interests in e-commerce, to note that the functions of such organizations are analogous to the services provided by passport issuing agencies now; to verify identity and to issue a passport that can be trusted.

III.3 Key issuance and certification is therefore carried out today by means of so-called Certificate Authorities (CA's), namely entities with high standards that are trusted by many other entities and organizations to a) do sufficient checks on the individuals applying to certify identity, and b) issue and manage keys in a proper and secure manner. To do so, CA's issue ***digital certificates,*** or public key certificates, to verify identity and the public key assigned. See Figure A-6. These certificates contain data such as:

- Certificate Serial Number
- Issuer (CA)
- Validity from/to dates
- Subject or holder distinguished name
- Subject Public Key
- Digital signature for all information inserted by the CA

III.4 The concept of a verifiable public key and a trusted issuer is very important in Internet communications and e-commerce, and in fact is in widespread if often hidden use in everyday Internet activity today. These CA's maintain secure databases of the keys they have issued and maintain, and also publish (on their sites) Certificate Revocation Lists (CRL's) for those keys that have been cancelled or compromised for any reason and hence discontinued. Organizations using and relying on the public key of an entity, for secure communication with them using their public keys, or to check that the public keys used by them for digitally signing a transmission are proper keys belonging to them, must check with the issuing CA on a constant basis to confirm their currency and validity.

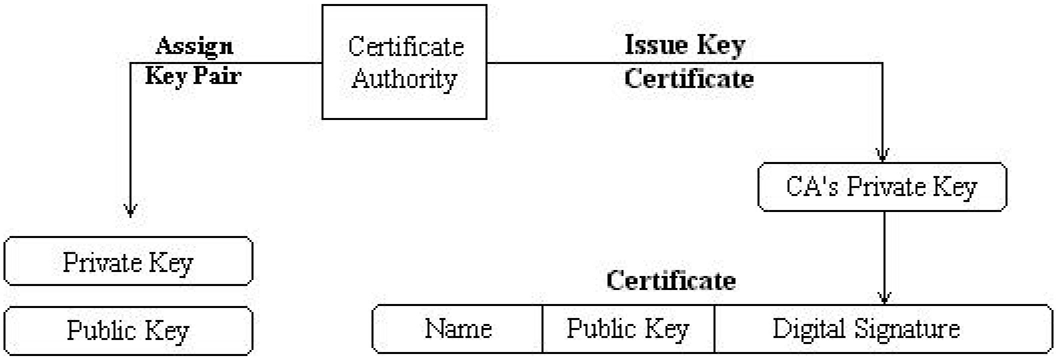

Figure A-6. The Role of a CA in Issuing Trusted PKI Keys

III.5 **Cross-Certification.** The existence of multiple CA organizations around the world has also created certain complex practices worthy of note for ICAO purposes. Specifically, to work together and rely on the certificates issued by each other, such organizations must *cross-certify* each other; that is to say, look at how each other operates, checks and verifies the identity of applicants, maintains physical and system security, manages keys and CRL's (Certificate Revocation Lists), manages trust with employees hired, uses PKI algorithms properly, and a host of other factors.

III.6 This cross-certification effort is essential for the commercial infrastructure of PKI to operate. In order to carry it out effectively, there has developed significant practices in the CA industry to formalize their *operating policies* and their *operating practices* into written documents, like detailed standards or policy manuals that must be rigorously followed within the CA organization. These are formally referred to as "Certificate Policies" (CP's) and "Certification Practice Statements" (CPS's). Typically CP statements are open and reviewable by other CA's who, through a process of mutual audit and review, can determine that the CP is sound and that the CA that has adopted it is in fact able to carry it out. The actual method of carrying out the CP is the subject of the CA's CPS, referring to the "how" of the CP. The CPS is often a secret or private document, as revealing the methodologies used to keep secrets secure on its computer site, for example, might yield clues as to how to hack into the system and cause serious damage.

III.7 Many CA organizations, and countries who have initiated PKI for their own purposes and to permit effective communication with their populaces, have devoted considerable effort to defining CP and CPS standards for their own purposes. These documents are often very extensive, and are beyond the scope of this Technical Report to detail. Any country wishing to implement the applications contained herein will inevitably require professional assistance in the structuring of acceptable practices for their own purposes, but this is becoming more commonplace in the world today as the benefits of PKI and better understood by governments. Readers may reference several sites for access to typical CP's, one very robust example being the Canadian one, available at http://www.cio-dpi.gc.ca/pki-icp/guidedocs/cert-policy/.

III.8 **CA Hierarchies.** Another important means of ensuring the validity of certificates and trust in the issuing CA, and also for ease of cross-certification in some instances, is the organization and recognition of CA's into hierarchies, where higher-level (and presumably more trusted) CA organizations certify those CA organizations under them. Such a structure may be utilized in a variety of situations; for example, a distributed organization may certify the issuing status of distributed CA entities within its own structure, perhaps at different geographical locations or for different subsidiaries, al under the overview and certification of the organization's central authority. Similarly, a passport issuing agency may permit different issuing offices to act as CA for the issuance of certificates to passport holders (this application is discussed in later sections), or a country may have a centralized CA for all of its issuing agencies and so will certify the ability of its passport issuing agency to issue keys and certificates.

III.9 This hierarchical approach is effectively implemented for the outside world through the use of signed certificates in a manner equivalent to that described for individuals. In other words, the private key used by each CA in the hierarchy to digitally sign the certificates issued by it, and the public key used by the outside world to verify the signed information, are themselves issued and certified by a parent CA. This parent CA actually issues a certificate to certify the public key of the lower CA, and this chain or hierarchy can continue upwards through several levels, as shown in Figure A-7. The checks on the validity of public keys carried out by an outside entity must in fact proceed up this chain, checking each certificate in turn, to provide true security for the transaction in question, obviously imposing practical limits on the number of levels implemented.

III.10 Ultimately in such a hierarchy the chain must stop. At this top level there lies what has been referred to as "Root Certificate Authority" or "Registration Authority" (RA), namely a CA of the very highest level of trust that is presumably recognized as such by most other entities. In the case of countries it may be the most senior level of security service or police in the country, whereas in organizations it may be a centralized and very widely trusted organization. This RA level must, and does, self-sign its own certificates at the top of the chain, and so ultimately this is where the buck stops as far as verification of public keys is concerned. The level of trust must be very high here, for both certificate validation as well as cross-certification and recognition of the CA organizations lower in the hierarchy, or the whole structure of trust will be invalidated.

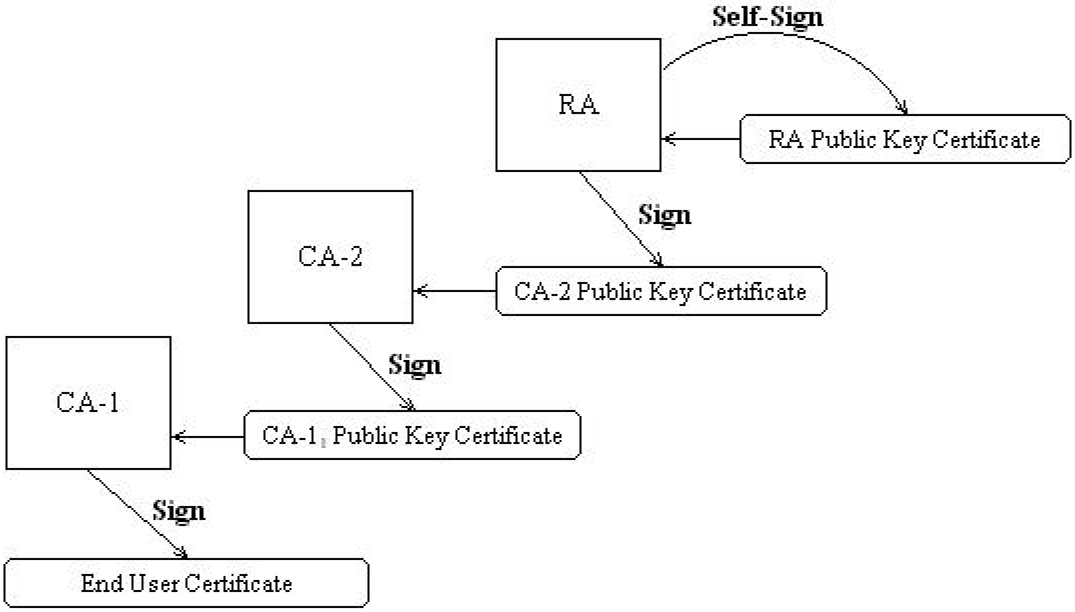
Self-Sign
RA
RA Public Key Certificate
Sign
CA-2
CA-2 Public Key Certificate
Sign
CA-1
CA-1 Public Key Certificate
Sign
End User Certificate

Figure A-7. Sample Hierarchy of CA Organizations and Signed Certificates

III.11 Some knowledge of PKI technologies and infrastructures, as presented in this Annex, is essential for understanding the methodologies proposed in the main body of this Technical Report. Further explanatory information is available through the references section herein.

Annex "B"

Use of the LDS for PKI-Enabled Digital Signatures on MRTDs

I. LDS Compatibility with ICAO PKI.

I.1. The proposed PKI application for Digital Signatures is accommodated by the LDS specifications. This Annex is intended to demonstrate the specifics of DS insertion, particularly on present forms of MRTDs, as described by the LDS. These present MRTD forms will typically use the LDS Sequential Specification.

I.2. The sequential file format specification is of the following form:

{Header}{DGPM}{MRZ Data}{Opt DG$_1$}..{Opt DG$_n$}{Dig Sig}{Opt PTN}

where:

{Header} = * {AID} or Application ID in ISO format Annnnnnnn (pix)
* Version level, recorded as "Vxx", presently "V00"
* Total LDS length (less header and length spec)
{DGPM} = Data Group Presence Map, comprising 2 bytes or 16 bits
{MRZ Data} = MRZ data repeated
{Opt DG$_n$} = An Optional Data Group
{Dig Sig) = The digital signature for the data file, per this TR$_{PKI}$
{Opt PYN} = Optional Person To Notify, not included in the DS

I.3. The AID must be submitted to ISO/IEC for number assignment, and the "pix", or application suffix, is assumed to be "01". The 9-digit application ID is mapped into hexadecimal characters. For purposes of example here only, the AID shall be assumed to be (in hexadecimal code) "A0 00 12 34 56.01"

I.4. The LDS length specifications are presented in ASN.1 length encoding rule format. These are as follows:

LENGTH RANGE	# OF BYTES	1ST BYTE	2ND BYTE	3RD BYTE
0 – 127	1	Binary Length	N/A	N/A
0 – 256	2	"81"	Binary Length	N/A
0 – 65,535	3	"82"	Binary Length	

Table 1 – Data Length Encoding Rules With ASN.1

Therefore, for a length of 800 characters, or a hexadecimal value of "03 20" in 2 bytes, would be recorded as "82 03 20" in 3 bytes using the above notation.

I.5 The DGPM is a 2-byte representation of the presence of optional data fields, each marked by the presence (“1”) or absence (”0”) of the corresponding bit. The table values are as follows:

DG1 – MRZ (always required)
DG2 – Facial biometric template
DG3 – Finger biometric template
DG4 – IRIS biometric template
DG5 – Not used
DG6 – Displayed (compressed) portrait image
DG7 – Displayed (compressed) fingerprint image
DG8 – Displayed signature image (an image of the bearer signature, not a DS)
DG9-11 – Special machine-assisted security features
DG12-13 – Additional personal information
DG14 – Not used
DG15 – Digital signature. Always required for authentication.
DG16 – Person To Notify. This is not included in the digital signature.

I.6 These table entries are represented by bits starting from the left (most significant bit) and proceeding to the right (least significant bit) over the 2 bytes. Hence, in an ICAO DS authentication scheme using a face image, the minimum data group presence map containing MRZ, compressed portrait, and digital signature, would be:

”1000 0100 0000 0010” or “84 02” in hex notation.

I.7 The standard structure within the above elements varies with the elements themselves. For the compressed portrait (Data Group 6), the specification calls for the possibility of several images, which is impractical for printed or limited-space applications. Therefore the specification for this Data Group, for the sequential file specification only, is proposed to be modified to use the following hex codes:

”5F 64” = tag for data Group 6 (facial portrait)
”xx xx” = compression algorithm indicator.
”82 nn nn” = length of compressed image or portrait, per ASN.1.
”mm..mmm” = compressed portrait binary data

The compression algorithm indicator is important because of the likelihood that JPEG2000 and others may simply not fit within the limited data areas of current MRTD forms. While the use of private sector schemes is generally to be avoided, some may have to be adopted or permitted on an interim basis in order to proceed with DS authentication using compressed photo images for existing forms of MRTDs.

I.8 Should ICAO decide on one or more standard biometric templates or algorithms, the structure of these elements for the sequential specification above is to be found in referenced document (footnote 7). For example, for a fingerprint template, the DGPM would change with an extra bit to make it:

”1010 0100 0000 0010” or “A4 02” in hex notation

and the data structures and tags for fingerprint biometrics would be incorporated into the sequential file format.

I.9 The specification for the digital signature in footnote reference 3 is as follows in hex notation:

”B7”	= tag for Data Group 15 (static data signature)
”nn”	= length of signature, one byte, per ASN.1 length spec.
”xx”	= algorithm identifier
”kk”	= key ID
”bb..bbbb”	= Digital Signature

The length of the signature depende on the PKI algorithm, and will likely either be 40 bytes for DSA or ECDSA encoding, with a length specification of “28” in hex, or 128 bytes for RSA, namely a length specification of “80” in hex notation.

I.10 **Example.** The following is an example, with notes, to demonstrate what the LDS sequential specification will look like in a typical situation. The example assumes a compressed photo DS authentication scheme with an ECDSA digital signature, with a compressed portrait of length 500 bytes. The actual data assumed for the example is as follows, based on a similar example in the reference at footnote 3, with explanatory notes. Note that the check digits of the MRZ are arbitrary and are not actually calculated in accordance with 9303 standards.

Doc Type	= P
Issuing State	= CAN
Name	= Johann T Gutenberg. Length 19 with < char’s (hex 13)
Document #	= 789123456
Check digit	= 1 (arbitrary)
Nationality	= CAN
DOB	= March 17, 1965
Check digit	= 2
Sex	= M
Date of Expiry	= January 1, 2006
Check digit	= 3
Optional Data	= none
Check digit	= 4

In addition, for the portrait image, the following codes are assumed:

Compression algorithm ID	= 00 07 (arbitrary)
Compressed image length	= 82 01 F4 in ASN.1 hex, or 500 in decimal

Finally, the data elements assumed for the digital signature are as follows:

Length of signature = 28 hex, or 40 decimal (ECDSA)
Algorithm ID = 03 (arbitrary, for ECDSA)
Key ID = 01 (arbitrary)

The sequential LDS fields to be included in a “BLOB” area on an MRTD, such as a passport using a 2D bar code on h data page, for example, would therefore appear as follows Note that spaces are not part of the data field, but are only inserted here to separate fields for clarity in understanding.

A00012345601	**V00**	**82066C**	**8402**
Application ID	Version	Overall Length	DGPM

P<CAN13GUTENGERG<<JOHANN<T7891234561CAN6503172M0601013
name length

5F6400078201F4	**mm..mmmmmmm**	**B7280301**	**bb..bbbbbbbbbbb**
portrait header	portrait - 500 bytes	Signature Hdr	Digital Signature- 40 bytes

I.11 The above information and examples have been presented to illustrate practically how the generalized LDS specifications for sequential file formats can be utilized for development of proposed MRTD DS authentication schemes. The example applies to present or limited-memory forms of MRTDs, and similar applications using non-sequential formats will also store the above BLOB information, plus other biometrics and full ICAO PKI Certificates.

I.12 The full specification for the LDS, for all forms of MRTDs, will be reviewed and possibly updated to accommodate the proposed implementation of Digital Signatures. But the DS application is compatible with the LDS.