TAG-MRTD/15
WP/10
27/4/04
(English only)

TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS

Fifteenth Meeting

(Montreal, 17 to 21 May 2004)

Agenda Item 3: Report of the New Technologies Working Group (NTWG)
Agenda Item 3.1: Update on development of specifications for the use of PKI digital signatures for MRTDs

FREQUENTLY ASKED QUESTIONS ABOUT TECHNICAL REPORT ON PKI FOR MRTDS MARCH 2004

(Presented by the New Technologies Working Group (NTWG))

1. What is the objective of the ICAO PKI initiative?

The ICAO PKI (Public Key Infrastructure) initiative is intended to provide standards and a simple international infrastructure to support digital signatures applied to Machine Readable Travel Documents (MRTDs). These digital signatures are intended to permit authentication of basic data stored by the issuing State in advanced document storage devices such as Integrated Circuit Chips (ICCs) contained within the MRTD. This stored data includes the Machine Readable Zone (MRZ) of the passport plus digitized biometric measurements and other relevant personal data of the bearer. Using the digital signature, States receiving States can verify that the stored data is authentic; namely generated by the issuing State, and has not been changed.

2. Why is it necessary to secure electronic data?

Just as physically readable data such as the MRTD data page is secured from wrongful alteration or substitution by strong physical security features, data stored electronically on an ICC embedded into a MRTD must be protected against alteration and manipulation. One of the most effective ways of doing this is using Public Key Cryptography to digitally sign the data stored on the chip. Only the issuing State has knowledge of the private key used to do so, so States using the corresponding public key to check the digital signature know that the data was placed there by the proper issuing State and has not been altered.

(10 pages)

3. Why introduce a PKI scheme for MRTDs? Is there an alternative?

With an RFID (Radio Frequency Identification) chip placed within an MRTD, the power and functionality of digital signatures are ideal for protecting the data stored on the chip.

Other alternatives to PKI would require different technologies such as the Optical Memory Card (OMC), which is a Write-Once-Read-Many ("WORM") technology. Data written to the optical area cannot be altered and so needs no digital signature. OMCs have been implemented in several ID applications but were deemed not preferable by ICAO member States, who wished to augment present paper-based printed MRTDs (passports and visas) with new electronic technologies.

4. How will the ICAO PKI initiative operate?

As described in the Technical Report, each State will install at least a basic secure PKI infrastructure for the sole purpose of applying digital signatures to the data stored on the chips of the MRTDs it issues. These digital signatures will be used in accordance with ICAO international standards regarding algorithms, key lengths, hashing methods, key lifetimes, and other standards and practices described in the Technical Report.

Each State will share the public keys that they use for signing MRTDs with all other nations by forwarding public key certificates to the ICAO Public Key Directory (PKD), accessible by all nations. States may also opt to include the public key certificate for the MRTD signature on the MRTD chip itself. These public key certificates are signed by each State's internal CA (Certificate Authority) established for this purpose, and whose own CA public key certificate, a fairly static one, is shared directly with other nations through diplomatic means.

5. Will each passport holder have his or her own certificate?

No. There is no intent on the part of ICAO member States to issue and manage individual MRTD-holder certificates. Only individual States will have keys and key certificates in the ICAO initiative, which makes the whole structure much easier to manage and maintain.

There is an option in the Document Security Object (see the Technical Report) to include a document-specific key for Active Authentication of the chip; although this optional key pair is tied to that MRTD and therefore to the holder of the MRTD, this key pair is only used for authentication purposes.

6. Will individual passport holders be able to read the digitized data on their own MRTDs?

Many States will implement passive chip MRTD applications (i.e. with no access control), and data on these chips could be read with an appropriate RFID chip reader. Even chips with Basic Access Control, as defined in the Technical Report, could be read with knowledge of the MRZ and the access method used.

Nonetheless it is unlikely that individual MRTD holders will want to do this, and do the work necessary to make sense of the data read. The data content could be interpreted with a little effort from the encoding method used on the chip and a knowledge of what appears on the data page, but access to detailed specifications such as are contained in this Technical Report and the ICAO

Technical Report for the Logical Data Structure (LDS) would certainly help. The PKD, an open access Internet facility, could also be accessed by the MRTD owner to determine the public key needed to verify the digital signature, although a detailed knowledge of how the hash is calculated would be required as well. Anything protected on the chip with unknown keys, such as additional biometrics stored using extended access control or data encryption, could not be interpreted.

So the question is really why the MRTD holder would want to do this. Many States, perhaps as a result of privacy legislation, will decide to advise holders of chip-enabled MRTDs on what the nature of the stored data is. Whether this is done by a printout of the actual data stored or simply a statement of what types of information are stored there and why, is up to individual State policy.

7. What mechanisms are used to protect the privacy of the data on the MRTD ICC?

The ICAO PKI application involves the use of proximity RF (Radio Frequency) ICCs, namely computer chips that are readable by contactless RF communications at very close range. Although eavesdropping on an existing communication between a reader and a chip is possible in a larger distance, some States consider the risk of eavesdropping in real operational circumstances to be very low, and with little negative impact should the data somehow be eavesdropped. Other States differ greatly on this point, and will protect their data from any such eavesdropping or inadvertent capture.

Where States wish to protect against eavesdropping on transmitted personal data, they can implement the Basic Access Control mechanism described in the Technical Report. The method proposed involves using a key derived from the MRZ which therefore must be read from the data page, hence proving that the passport bearer voluntarily proffered the document for reading. Once the authentication challenge is accepted, data is transmitted using session keys that are set up between the MRTD chip and the reader to encrypt the communication between reader and chip.

8. How will other biometrics such as fingerprint and iris-scan be accommodated?

Other biometric measurements (fingerprint, iris) are considered sensitive for privacy purposes by ICAO member States, and as such need not be made available in open format, even with Basic Access control. As such, these biometric measurements are to be protected with Extended Access Control or data encryption by each nation wishing to capture them.

Some States will capture and store these biometrics in conjunction with partner nations for private bilateral or n-lateral schemes where this information can be shared within this group of partner nations.

ICAO is not proposing any PKI or other encryption standards with regard to these biometrics. Other ICAO Technical Reports deal with the interoperable formats of these biometrics, if used, and the LDS locations for their storage.

9. Why is the ICAO Public Key Directory necessary?

The ICAO Public Key Directory is the most efficient way to distribute and manage the international set of signing certificates and keys that will be used by all participating States to authenticate MRTD chip data. While the appropriate Document Signing Key certificates may be placed on the MRTD chip itself, the PKD also provides very important operational safeguards and access features desired by the ICAO community.

Firstly, regarding county procedures, the ICAO PKD facility provides important information on the number of keys that each State has in existence at any time, and provides assurances that these key certificates are known in advance by all other member states, that these certificates are properly set up with appropriate validity dates representing the lifetimes of the documents signed, and that these certificates have not been backdated or duplicated. These matters are part of the due diligence performed by ICAO on new key certificates forwarded to it.

Secondly, the PKD may discourage the malicious generation of a "rogue" key certificate, for example one that might be generated internally by a corrupt official with access to the State's CA key (such a rogue key might be used to sign a single improper MRTD, for example). The existence of the PKD limits the flexibility to do this if this certificate must be posted to the PKD in advance, be scrutinized by both ICAO and authorities in the issuing State (who will see the suspicious certificate in advance).

Thirdly, the PKD represents the only access that airlines and other legitimate non-government users have to such certificates. Although it is recommended to store the Document Signing Certificate on the MRTD chip, it cannot be counted on to be there. In addition, airlines will require the added confidence of certificate presence in the PKD, representing satisfactory completion of ICAO due diligence and the lack of any certificate revocations.

These benefits are above and beyond and additional to the strong security provided by the PKI technology used for digital signatures, and are important to the secure and successful operation of the ICAO PKI initiative.

10. Will airlines be able to read and authenticate chip MRTDs?

The PKD will be a totally open and Internet-enabled resource, available to any and all who wish to access it (for read-only). The lack of user sign-up protocols will lead to simplification of implementation, and broader security through the ready availability of its certificate services to airlines and others who wish to use it to validate documents. This is particularly important to airlines, who will want to take advantage of the MRTD chip data and digital signature to authenticate the MRTD before passenger boarding, and to confirm that such checks have been done for Advanced Passenger Information (API) requirements.

11. How many keys can a State use for signing at any time, and how often are they changed?

More than one signing key may be used by a State at any time. The number and the signing lifetime of these keys is really determined by balancing two factors: the need to limit the number of MRTDs issued and signed by each key, and the need to limit the number of keys that must be managed by the PKD and every State's border system. Signing too many documents with the same key exposes more

MRTDs to the event of a compromise of that key, whereas the use of excessive numbers of keys makes the international task of key management very burdensome.

ICAO recommends therefore that States not use the same key for more than several hundred thousand documents although there is no rationale for fixing this number to precise levels. In addition each such key should change every three months, even if the number of documents signed by each is limited. It is up to each state to determine what works best for them given their document issuance counts and other factors.

12. **How will States obtain up to date public keys of all other States from the ICAO Directory?**

The PKD will not be designed or implemented for active on-line real-time key confirmation for every MRTD encountered at every border post in the world. Rather States will be expected to download the entire copy of the PKD, estimated to be <25MB, on a regular basis and store it internally in their border management systems. In this way chip data stored on MRTDs encountered can readily be authenticated from the appropriate issuing State public key certificates stored in the PKD downloaded copy.

13. **Will States update and maintain the PKD or will ICAO update and maintain the PKD?**

States will regularly provide new Document Signer Certificates to ICAO, but it is essential that ICAO exercise some due diligence over the process on behalf of member States (see Q 9). Therefore all proposed updates forwarded by States will first be used to modify an "update" PKD which is read-accessible only by ICAO. Once ICAO has examined and accepted the proposed updates they will be copied into the public read-only PKD available to all States and other users.

14. **Will ICAO sign the certificates after their due diligence when they post them to the public PKD?**

ICAO will not sign any certificates stored on the PKD, nor sign any PKD certificate downloads by States, so as to not give the impression that it is in any way acting as a CA for these certificates. Communications with the PKD for downloads and certificate requests will be secured through SSL (Secure Sockets Layer), which will involve an ICAO key for session encryption. To further protect against any wrongful insertion of other certificates into the PKD, or into a PKD copy downloaded by any State, ICAO will also develop data control checks and statistics, such as record counts by nation, overall sizes, and similar data integrity controls for the current PKD version, which it will sign before transmission to States for their own PKD version validation after download.

15. **Does the ICAO PKI use CRL's, and if so how will they operate?**

CRL's (Certificate Revocation Lists) will be used in the ICAO infrastructure, but hopefully will seldom be necessary due to compromise of a Document Signer or State Signing CA private key. Nonetheless "good PKI practice" involves the posting of a CRL list, even if there are no revocations, on a periodic basis and so is mandatory for the ICAO application.

The primary channel for CRL distribution is by n-lateral communications between states, with the ICAO PKD being the secondary, but mandatory, channel. The primary channel is essential for CRL's necessitated by key compromise events; these CRL's must be shared between and amongst States by urgent messaging, and is the responsibility of the State with the compromised key. However, in the event that the periodic CRL list from a State contains no revocations, then the State would not use the primary n-lateral channel of communications and would use only the secondary channel, the PKD.

Certificates do not become invalid after the keys' usage period for signing is over (3 months maximum). This is due to the fact that the documents signed by that key remain valid for a long time (10 years?); the certificate must therefore also remain valid and unrevoked for that period of time. Each receiving nation must check that the Document Signer Certificate and the State Signing CA Certificate required to validate the signature on the Document Security Object are both still valid and have not been revoked. Therefore any CRL issued to revoke a certificate, or CRLs issued with no revocations (to establish that the certificate has not been revoked), must also remain in the Directory for the full lifetime of that certificate.

At some point beyond certificate lifetime, these certificates will be removed from the PKD as a matter of Directory cleanup. This would be done through some positive action by the issuing State.

CRL's will not be issued on the MRTDs of departing travelers. CRLs will only be shared bilaterally through the primary channel, and through the ICAO PKD.

16. **When would a Border Inspection Point use the public key stored in the MRTD chip as opposed to a public key from the PKD?**

If a border inspection point encounters an MRTD signed by a key where the corresponding certificate is not present in the PKD copy currently stored by the State, this may imply that recent PKD updates, including any CRLs, have not been captured by the State. This is a situation that should be reviewed in accordance with the policy of each State. One alternative is to forward a special real-time request for specific certificate and CRL information to the ICAO Directory. Alternately, if the public key certificate is also contained on the MRTD chip, duly signed by the State's CA, the receiving State may opt to accept the new key without ICAO PKD reference. States thinking of accepting MRTD chip certificates as a general practice, however, should consider that the verified existence of these certificates on the PKD provides many additional due diligence safeguards and operational security features of benefit to the ICAO community.

17. **Is the ICAO PKI application patent-free?**

The ICAO PKI application has only one known patent issue; namely the methodology described in this Technical Report regarding Active Authentication. Arrangements have been made with the patent holder so that this technique will be available to ICAO and all participating States on a royalty-free basis; in any case the use of this technique is optional in the ICAO application. All other areas of the ICAO PKI are believed to be patent-free, including the Basic Access Control technique described in this Technical Report.

18. **Would it not be simpler to adopt a single algorithm for ICAO usage?**

The use of one select algorithm may make implementation slightly simpler but is impossible to mandate, as several States already utilize different algorithms in their PKI implementations. This might also pose some security difficulties in future, if one algorithm was found to be less secure or more open to attack than others. As a result DSA, RSA, and ECDSA are all permitted digital signing algorithms for use in the ICAO PKI initiative. None are recommended as the default; it is up to individual States to determine which best suits their needs.

19. **Is SHA-1 acceptable for this application?**

As described in this Technical Report, SHA-1, SHA-256, and SHA-512 are all permitted hashing algorithms. ICAO recommends the use of appropriate SHA algorithms consistent with good PKI practice for the key lengths required.

If SHA-1 is to be used, States are advised to pay particular attention to the possibility of cryptographic "birthday attacks", particularly if a State accepts MRTD photos in the form of digitized images. In this case States are strongly advised to add entropy (add additional information bits) to the digitized photo received before carrying out the SHA-1 hashing process.

20. **If keys are only to be used for signing for a short period, how long will they remain valid?**

As described in this Technical Report, even though Document Signer private keys may be used for signing for only a short period (3 months for example), they must remain valid for the longest lifetime of any MRTD signed. See Q 15. Similarly, in accordance with PKI practices, State Signing CA Certificates must remain valid for the longest lifetime of any Document Signer Certificate issued.

For example, if a Document Signer Private Key is used for three months to sign 10-year validity passports, then the lifetime of the corresponding Document Signer Certificate is 10 years plus 3 months. Similarly if a State Signing CA Private Key is used for 3 years to issue Document Signer Certificates that will each be used for 3 months for signing of 10-year validity passports, then the lifetime of that State Signing CA Certificate is 3 years plus 10 years plus 3 months.

Variations on these lifetimes may occur in unusual circumstances, such as when MRTDs are issued in advance of their validity dates. For example, some states may issue a passport to a person about to get married and change their surname, with a start validity date up to three months in the future. This will effectively extend the certificate lifetimes by an additional 3 months. States must take care to assign the proper validity date ranges to such certificate to avoid difficulties in the future with certificates inadvertently becoming invalid for still-valid MRTDs.

21. **With such long key lifetimes, does ICAO feel the key lengths chosen will remain secure over these periods?**

In determining appropriate key lengths ICAO had to consider the long periods of time that MRTDs remain valid, which could be up to 10 years (see above). In view of this key lengths must be such that they are not likely to be compromised through brute force efforts even in that time period.

Although there are no definitive answers to these cryptographic questions, ICAO has adopted key lengths that are very robust based on NIST documentation and other expert sources.

22. **What is the minimum ICAO PKI implementation that a State may carry out?**

As described in the Technical Report, the minimum implementation that a State can carry out would involve issuance of a chip-enabled MRTD with no access control, no active (chip) authentication, and containing a facial recognition biometric measurement in accordance with ICAO specifications. The face recognition data would correspond to the photo on the MRTD data page or visually readable area.

The border inspection facilities of each State should, however, be equipped not only to read and verify its own MRTDs but also those of other States; this would include, as a minimum, MRTDs from those States that use Basic Access Control mechanism to read chip data. The inspection points must also accommodate all hashing algorithms and digital signature algorithms that are permitted. Active Authentication, as described in this Technical Report, is not required in a minimum implementation at border inspection points.

23. **What methods are allowed for Extended Access Control? Will border inspection stations have to have additional complexity to utilize it?**

Extended Access Control applies to chip data that is protected other than through data encryption. This applies specifically to biometric measurements such as fingerprint and iris images and possibly other data the issuing State may wish to insert. Such data is intended for use only by the issuing State or by a group of States in a private n-lateral agreement; as such the access protection technique and private master keys used are a matter for the State or the group of States to decide (see Q 8). If these access methods use different techniques from those contained in the Technical Report then it follows that the border inspection points of these States must also be able to carry out the access computations to read and interpret this information in addition to regular ICAO PKI requirements.

24. **Will States need a national PKI security infrastructure to generate State CA root and other ICAO keys?**

This is a matter for each State to decide. Operationally, for ICAO purposes, it is not necessary; a small scale PKI infrastructure could be implemented, with appropriate safeguards and key protection facilities, for the sole purpose of generating and managing keys and certificates for MRTDs, and signing MRTDs issued.

25. **What security decisions will issuing authorities need to make when developing an electronic passport?**

Developing an electronic or chip-enabled MRTD requires consideration of many security aspects. Firstly there is the important matter of what the PKI infrastructure for MRTD issuance must constitute, complete with appropriate best practices for key management and access control, root key generation and protection, in-State communications security, and the like. (ICAO intends to develop or adopt appropriate best practices documentation to guide States in this regard.) In addition, however, there are many other PKI security decisions that must be made: should the basic chip data on the MRTDs issued be protected with Basic Access control? Should the MRTDs be protected against chip copying or substitution with Active Authentication? Should additional biometrics be included and protected by Extended Access control? These choices are all described in the Technical Report.

In addition there are also a number of very significant physical security decisions that must be made. These involve the actual method of inserting a chip in the book or MRTD and protecting it from substitution or operational failure over the intended lifetime of the MRTD. These matters are outside the scope of this Technical Report; reference is made to other ICAO Technical Reports and documentation in this regard.

26. **What happens if a State's Document Signer Private Key is compromised?**

When a compromise of a Document Signer Private Key is detected, the State must immediately issue a revocation, to be communicated to (all) other States, and to ICAO PKD, within 48 hours maximum. See Q 15.

All documents signed by that key will then not be able to be validated using their digital signatures, and so these document must thereafter be inspected on first principles. This may result in significant delay and difficulty for the bearer if the world by then has increasingly come to rely upon the encoded data, with biometric, and the digital signature to verify the authenticity of the document and the bearer.

27. **What happens if a State signing CA Private Key is compromised?**

Compromise of a State Signing CA Private Key is a disastrous event for that State. In effect, revoking that key invalidates all of the MRTD signatures applied by any Document Signer Private Keys whose corresponding certificates were issued by that State Signing CA Private Key.

To issue new documents the State basically must start over: generate a new State Signing CA Certificate, share it via diplomatic means with other States, begin to issue new Document Signer Certificates, post these with the ICAO PKD, and begin to sign passports and MRTDs with these new keys.

28. **Will the chip serial number be part of the certificate extensions?**

The chip serial number may be stored by a State in the LDS Data Group 13, where it is protected by hashing and digital signing of the hash. This data will not necessarily be used by other States and is not standardized. The ICAO PKI Active Authentication scheme (see below) is intended to provide protection against chip copying and substitution.

29. **How can the chip be authenticated as the proper one originally encoded by the issuing State?**

As described in the Technical Report, the ICAO PKI also utilizes an optional Active Authentication Key pair, which is a document-specific key pair. This key pair is entirely contained on the chip, the private portion within the chip's secure memory, and the public portion in LDS Datagroup 15. An inspection station may opt to use these keys along with a hash value taken from the MRZ to verify that the chip is genuine and belongs to this MRTD.

These Active Authentication Keys are document-specific and are not subject to international distribution, control, or CRL reporting. They also do not restrict the retrieval of open data from the chip without performing Active chip Authentication.

30. **Will the ICAO Public Key Directory be ready in 2004 and how much will States pay for its setup and on-going operation?**

The ICAO PKD is intended for implementation by October 2004. All funding of PKD implementation and operations is to be achieved through annual participation fees from States that are issuing documents with digital signatures in accordance with ICAO international practice.

The ICAO PKD will be an open and accessible facility. Airlines and other users who require steady access to the PKD will be encouraged to access copies of the PKD on a regular basis, just like the border inspection agencies of member States. It may not be possible to charge airlines and other users for this service given the open Internet architecture of the PKD; however there are clear security benefits in security for all nations in encouraging airlines and other agencies to use the PKD to validate digital signatures and documents.

Exact fee structures and rates have not been finalized at this time.

— END —