Electronic machine-readable travel documents (eMRTDs) – The importance of digital certificates

Superior security

Electronic machine-readable travel documents (eMRTDs) are well-known for their good security. But the correct use of digital certificates in these documents is the difference between good security and superior security. Georg Hasse and Michael Schlüter of secunet Security Networks AG report.

The truth about security

When you hand your passport over at a country's borders, you assume the control staff knows what they are looking for. Sadly, this isn't always the case. They know that ePassports store the passport holder's data as data files on the chip. They may also know that data access is protected by access control mechanisms, while data integrity is protected by a digital signature supplied by the passport provider. However, what many border authorities do not realise is that if they don't perform full certificate checks to ensure the document signing certificate is from a trusted source, they could be letting a functioning passport that has been falsified pass through their borders.

Additionally, some authorities do not know about passive authentication (PA), so they haven't introduced checks at the border. PA detects if the passport chip data has been modified. The chip holds a file that stores the hash values of all the files it contains (such as the passport-holder's picture and fingerprints) and a digital signature of these hashes. The digital signature is made using a document-signing key, which itself is signed by a country-signing key. If a file in the chip (for example, the picture) is changed, this can be detected since the hash value will be incorrect.

As the world's border control authorities move towards automated checks, it is paramount that robust checks are made to ensure the document isn't a fake and hasn't been altered in any way. Authorities need to understand the importance of implementing robust systems to ensure that the document is properly checked the moment it enters the destination country. This is particularly important in Europe, where entry into one country in the Schengen area automatically allows free movement between other states that are part of the scheme; just one weak border post could ultimately put the whole continent at risk.

Evolution of PKI

Many people are familiar with the general concept of public key infrastructure (PKI) technology. It has traditionally been used in internet transactions, where keys need to be trusted across a broad range of users and organisational entities. This has resulted in elaborate key certificate systems, where public keys are issued in certificates which are digitally signed by trusted issuing organisations called Certificate Authorities (CAs). This trust is further reinforced by higher level CAs as part of a trust hierarchy. It is also necessary to have Certificate Revocation Lists (CRLs), which indicate if a key (certificate) has lost its validity. By revoking a certificate and publishing this revocation in a CRL, the certificate's issuer informs receiving parties that the contents can no longer be trusted.

The International Civil Aviation Organization (ICAO) points out that its operating environment is different from these commercial ones. As a consequence, the ICAO has specified a customised approach, known as the ICAO PKI scheme. This specifies a two-layer certificate chain, enabling an inspection system to verify the authenticity and integrity of the data stored in the eMRTD's contactless IC. The root (highest level) CA in this scheme is the Country Signing CA (CSCA), which authorises Document Signers (DS) to digitally sign the Document Security Object (DSO) on the contactless IC. The CSCA certificate is distributed between states. The DS certificate is published on the global ICAO Public Key Directory (PKD) and/or stored on the eMRTD's contactless IC. CRLs are published on the PKD and exchanged between states.

The ICAO says its PKD acts as a central broker managing the exchange of certificates and CRLs. This central role is critical to minimise the number of certificates being exchanged, to ensure timely uploads and to make sure technical standards are adhered to, to ensure interoperability is maintained.

The nuts and bolts

The introduction of eMRTDs normally means including biometric data as well. Just like traditional optical data, this electronic data has to be secured against manipulation and unauthorised access. Usually, this protection is achieved by means of PKI mechanisms. The backbone of the security structure for eMRTDs consists of two comprehensive PKIs. While the ICAO-PKI ensures the authenticity and integrity of the documents, a second PKI, the Extended Access Control (EAC)-PKI, is needed for enhanced access security for more sensitive data such as fingerprints. The exchange of the required certificates makes modern border control highly complex.

When ICAO Doc 9303 – which contains the organisation's specifications for MRTDs – was initially published, it specified that CSCA certificates had to be exchanged between states without providing detailed specifications of how to achieve this. But during the first few years of states issuing ePassports, it became clear that the lack of such specifications produced a wide range of interpretations and inefficient processes.

To address this, the ICAO has published a technical report on CSCA countersigning and Master List issuance. This highlights an approach where countries create a list of received and validated foreign CSCA certificates. This so-called Master List is countersigned by each country and published via the ICAO PKD, to support the distribution of self-signed certificates between nations.

Trust

Only authorised organisations have access to the sensitive biometric data (such as fingerprints) stored in eMRTDs. Therefore, the requirements for access control and communication confidentiality have been specified within the EAC-PKI. The EAC-PKI describes the security mechanisms which allow an eMRTD to verify an access request by itself. To access eMRTDs from other countries, you have to be equipped with the corresponding rights. To obtain those rights, EU countries have agreed to accept the Czech Standard CSN 369791:2009 as the common communication protocol.

When looking for a PKI solution, you need to choose a supplier that can meet all the requirements for issuance, infrastructure and control. This includes the international exchange of certificates and other relevant information.

Whose responsibility?

The security of identity documents is the responsibility of everyone in the chain – from the organisation that issued them to the border control official who checks them and allows travellers to enter a country. The chain is only as good as everyone involved in it – and any weaknesses can be easily exploited by criminals.

Modern ID documents which digitally store personal data on an integrated RF chip make the prospect of automated border controls establishing mobile controls quite feasible. But before these new processes can be implemented, 194 states worldwide must exchange information – such as certificates – with each other and details of an estimated one billion flights per year, as well as land and sea travel. Each nation keeps a list of these certificates. For example, Germany's 15 August 2013 Master List contains 141 CSCA certificates and CSCA link certificates from 54 countries, and is also used by other countries.

ePassport PKI in a nutshell

Understanding how the various components of PKI technology work in ePassports is essential to understanding how and why it should be adopted.

The general access protection for the data stored inside the eMRTD is implemented by the BAC or PACE mechanism. Using these protocols, a secure communication channel is established and the data printed on the document is needed to access the data.

EAC-PKI

Extended Access Control (EAC) provides additional security mechanisms to ensure that only authorised organisations can grant access rights to Inspection System (IS) for specific sensitive eID data, such as fingerprints.

These access rights are granted by card-verifiable certificates (CVCs). Their three-layered infrastructure consists of a national trust anchor (Country Verifying Certificate Authority/CVCA) that is connected to authorised Document Verifying Certificate Authorities (DVCAs). DVCAs issue short-term IS certificates to the actual inspection system.

For international EAC certificate exchange, a centralized interface called the Single Point Of Contact (SPOC) has been defined. The SPOC receives certification requests from foreign countries and connects the DVCA to the corresponding CVCA.

ICAO-PKI

The authenticity and integrity of an eID can be checked by verifying the electronic signature. The ICAO has introduced the mechanism used for this validation: passive authentication (PA). A complete PKI with the CSCA as the national trust anchor and the DS as the document manufacturer has to be provided. The exchange of certificate data can be processed via the ICAO-PKD.

At secunet, we recommend that you select a partner that can supply ICAO-PKI-related products such as CSCA and DS services, as well as components which fulfil the requirements of the EAC-PKI, such as CVCA and DVCA services.

Speed

Checking certificate validity is a quick process. According to the results of Germany's EasyPASS automated border control scheme, the average time taken to read and check ePassport data using both optical and electronic checks is just five – six seconds. What's more, electronic document checks proved reliable, with less than 0.1% of travellers rejected due to the failure of the checking system. The availability of CSCA certificates is central to this. As those involved in the pilot point out, it is necessary to have a combination of different checks to ensure the border control process is secure, and fully checking eMRTD electronic security features ensures a high level of reliability.

The technology in action

The Latvian Ministry of Interior is renewing its existing PKI for ePassports and issuing new national ID documents. As part of this project, the PKI is being extended with a central infrastructure for checking the validity of these documents. As a result, the new system enables eID documents to be issued, and to be verified at border controls and Latvian consulates worldwide. The integrator is using a solution that provides the complete range of functions required for the Latvian national PKI: it includes the systems needed for issuing national identity documents that conform with international ICAO regulations as well as the EAC-PKI components used to verify international eIDs. The product's flexible design means it fully meets the specific requirements of the Latvian government, while at the same time providing a secure and reliable system.

Summary

The current document verification process shows the importance of comprehensive use of the security mechanisms provided by modern travel documents. In particular, it's essential to properly use the certificate infrastructure, which is vital for reliable and secure verification procedures (especially for passive authentication).

Dr. Uwe Seidel of the German Federal Criminal Police Office (BKA) puts it rather well: "A modern document verification process needs to comprise state of the art electronic and optical security mechanisms. The proper implementation of 'Passive Authentication' for proofing integrity and authenticity of electronic data is indispensable for a secure border control."

The main challenge to establishing a document verification infrastructure is still the international distribution of CSCA certificates. The Master List concept plays an important role in this process. It is still a time-consuming process for each country to collect and validate the different CSCA certificates. Even after the initial certificate exchange, it is important that countries are notified when a new CSCA certificate is used by a country before the corresponding travel documents are presented at the border.

At secunet, we believe a new approach could be the provision of an independent Master List by, for example, the ICAO or other international bodies such as the European Commission.

Contact

secunet Security Networks AG
Public Sector, Portfolio Electronic Identities
Mr. Michael Schlüter, Head of Software Development
Kronprinzenstr. 30
45128 Essen
Germany

Email: Michael.Schlueter@secunet.com

secunet Security Networks AG
Public Sector, Portfolio Electronic Identities
Mr. Georg Hasse, Senior Product Manager
Alt-Moabit 91c
10559 Berlin
Germany

Email: Georg.Hasse@secunet.com