Travel Documents & Security Mechanisms

In the last decade, many countries started issuing passports with electronic chips. Internationally accepted standard for given field is ICAO (International Civil Aviation Organization) Doc 9303 (electronic passports are specified in part 1, vol.2). Three security mechanisms defined by ICAO are: Basic Access Control (BAC), Passive Authenication (PA) and Active Authentication (AA).

The Basic Access Control, Passive and Active Authentication

The Basic Access Control mechanism prevents unauthorized access to data stored on the chip. This mechanism allows the setting-up of a cryptographic channel to prevent eavesdropping on communication between a chip and inspection system. In addition, BAC ensures that the inspection system may only read data from the chip, provided that the system contains selected data recorded in the optically readable zone on the passport's data-page. In this way, BAC prevents reading of the contents of contactless chips from the passports of random bystanders.

Passive Authentication (PA) protects the authenticity and integrity of data stored on the chip. This mechanism uses an electronic signature generated during the chip personalization phase (data entry). Although PA is an effective means to ensure the authenticity of data stored on the chip, this does not allow the inspection system to verify whether the system is communicating with the original chip or with a copy into which the counterfeiter might have entered unchanged data together with the digital signature read from the genuine passport (chip-cloning).

Protection against chip-cloning is provided by the third mechanism, Active Authentication (AA). This mechanism uses a challenge-response protocol based on asymmetric cryptography. During inspection, the chip uses its (unpredictable) private key to sign a bit string that has been chosen randomly by the inspection system. The inspection system verifies the signature using the public key read from the chip. The authenticity of the public key is protected by the above-mentioned Passive Authentication mechanism.

Chip and Terminal Authentication

In Recommendation TR-03110, two other security mechanisms were defined – Chip Authentication and Terminal Authentication, and their mutual application known as Extended Access Control (EAC). Chip Authentication (CA) is an alternative to the (optional) ICAO Active Authentication mechanism. CA is based on principles of the Diffie-Hellman derivation of a shared secret. This prevents a third party from tracking the passport holder, for which the AA can be misused, while providing a strong key to secure encrypted communication between the chip and the inspection system.

Terminal Authentication (TA) enables the prevention of unauthorized access to data stored on the chip. A challenge-response protocol is used to check the authenticity of the inspection system terminal. However, a weak link in the TA is expiry control of the Inspection System Certificate, as the chip is not continuously connected to a power supply and hence no continuously running clock is available to determine the current date. To determine the date, EAC uses an approximation mechanism based on the derivation of time from the most recent valid certificate taken from a chain of certificates provided by the inspection system.

EAC provides a higher degree of privacy protection for the passport holder than ICAO mechanisms, however, on the other hand, this places increased demands on the technical infrastructure which is currently not a globally accepted standard. Passports issued by EU Member States implement EAC mechanisms to protect access to sensitive data, e.g. digital representation of fingerprints of the passport holder.

Plaut Slovensko, s.r.o
Karloveská 34, 841 04 Bratislava
Slovenská Republika
Tel.: + 421 2 3215 1411
Fax: + 421 2 3215 1412
E-mail: info@plaut.sk
Web: www.plaut.sk