CRYPTOMATHIC
www.cryptomathic.com

High Speed Inspection

HIGH SPEED INSPECTION

Since the mid 2000s the deployment of contactless smartcard systems has undergone a revolution. The ICAO-standardised Machine Readable Travel Document (MRTD) specifications and their implementation by global states has become the largest single contactless card (ISO 14443) application in the world and also the world's largest PKI. The global investment and commitment is considerable.

The goals of this initiative include greater border security, cracking down on organised crime, illegal immigration and terrorism, and well as a host of other value-added features. However in the push for commencing live issuance of advanced passport technology, there is a danger that inspection technology will be left behind. Hi-tech electronic and physical security features count for nothing if they cannot be properly and regularly examined; whilst there is no strict timetable for the adoption of electronic border checks, the return on investment in ePassports is entirely dependent upon their widespread use.

The High-Speed Inspection Business Case

Unfortunately, the contactless interface to ICAO-compliant travel documents (and other forms of ID) places severe limitations on the achievable communication rates, and the generation of electronic passports which are currently deployed in the field do not have high performance chips. It can take as long as ten seconds to read out the entire data set from a typical Basic Access Control (BAC) ePassport. Furthermore, this inspection rate is dependent on a wide variety of environmental and circumstantial factors which are difficult to predict or control.

If the overall processing time becomes unacceptable, electronic inspection will have to be relegated to second or third line inspection, where an electronic read is only performed on traveller's documents already identified as suspicious. It becomes wholly impractical to electronically process every traveller without increasing man power to prohibitive levels. As the amount of biometric data stored on ePassports inevitably rises, with the introduction of second generation ePassports with fingerprints, iris codes, ten finger scanning etc, the problem will only get worse.

Instantaneous Inspection

Cryptomathic's high-speed inspection technology can solve the problems of poor and unpredictable read times for ePassport and identity card stock, yielding a factor four increase in speed of inspection in the average case. Using this technology, BAC electronic passports can be read almost instantaneously (in less than one second), regardless of the amount of data stored. It is particularly well suited for high throughput border control scenarios such as international airports, where speed of inspection is critical. There is no dependence on specific chip stock type, and the technique can be applied to documents already in the field. Such dramatic results are achieved through use of a specially

designed encrypted caching mechanism, which stores the bulk data held on the identity document (in the case of ePassports, the data groups 1-16), bypassing the need to transfer this data over the low speed smartcard communication link.

The data is encrypted with a key derived from the content of the identity document itself (See figure overleaf). Such a cache is typically pre-loaded with the biometric data of the deploying nation's ID holders, and rapidly accumulates cached data on all international travellers (or a chosen subset of travellers, whatever is preferred) on their initial visits.

Data Protection & Compliance

If such a cache was encrypted with a key held by each inspection system, the data would be in the hands of the inspecting nation; it would be at risk of abuse and the cache would have to comply with data protection legislation, and indeed there is a blanket ban within the EU on storage of biometric data retrieved from EU ePassports.

However, each cache entry uses a different encryption key which is stored on the identity document itself, thus the information remains in the hands of the issuer. The cache information is impossible to extract or abuse without possession of the physical document (which contains the same data anyway): each cache exists in an essentially "deleted" state until the real identity document becomes available again. Furthermore the cache can be configured to store only part of each biometric data group (e.g. 90%) whilst the remainder is read from the chip – making

Pravda.dk

KEY POINTS

High Speed Inspection

- Cut inspection time by a factor 4
- Read BAC ePassports in under 1 second
- Cost savings from reduced staff requirements
- Unique architecture ensures data protection compliance
- Special security measures for EAC-protected data groups
- Patent pending technology

Compliance

- Aids data protection compliance for all data
- Compliant with EU ePassport regulations for EAC data
- "Encrypt and Destroy" ensures data is not retained
- Cache data integrity assurance from existing infrastructure

Availability

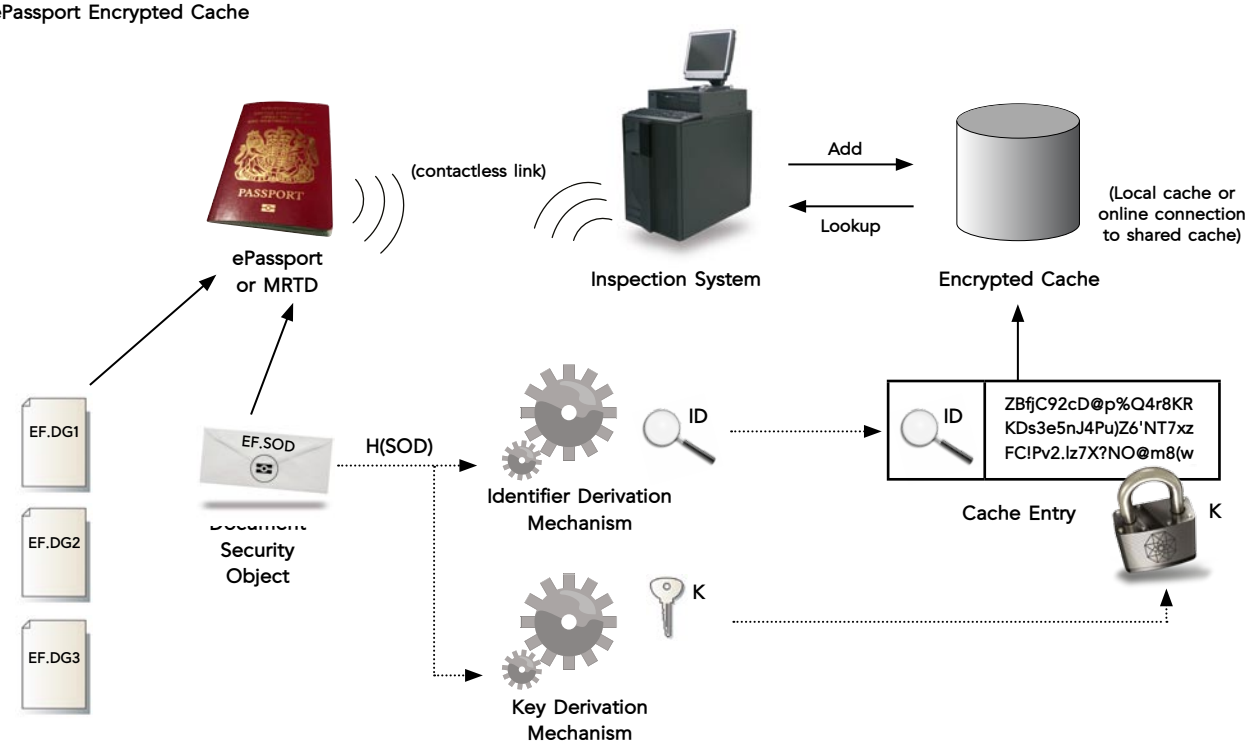
- ID Inspector SDK (+Cache Server)
- ID Inspector Mobile (+Cache Server)
- ID Inspector Server (+Cache Server)
- Standalone Cache Server (for use with own IS)
- Technology Licence

data clearly impossible to reconstruct even if the cryptography could somehow be bypassed.

The individual cache key is derived from high-entropy information within the Document Security Object (SO_D) contained in a BAC or EAC (Extended Access control) ePassport, and a pseudonymous storage and retrieval identifier is derived in the same way. Cache integrity is assured through the existing ID document integrity mechanisms of hashing and digital signatures, thus if any cache data is modified the inspection system retrieving the data will immediately become aware. Thus confidentiality, integrity and anonymity of the cache data are all assured.

Cryptomathic's high-speed inspection technology is patent pending, and is incorporated into the ID Inspector product range of inspection systems and software development kits. It is also available as a technology for third party licensing.

Figure: ePassport Encrypted Cache



ABOUT CRYPTOMATHIC

Cryptomathic is one of the world's leading providers of security solutions to businesses across a wide range of industry sectors, including finance, smart card, digital rights management and government. With 20 years of experience, Cryptomathic provides customers with systems for e-banking, PKI initiatives, card personalization, ePassport, card issuing and advanced key management utilizing best-of-breed security software and services. Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with an established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.

Learn more at cryptomathic.com