temporal
Secure Digital Identity

ePassport Extended Access Control

White Paper

1 INTRODUCTION

As ICAO[1]-compliant ePassports come into widespread use in Q4 of 2006, it is an appropriate moment to review some of the initiatives required for the next stage of development. In an initiative as ambitious as ICAO's ePassport, it was necessary to start with a relatively simple implementation and build on this in a series of phases.

The first phase added a contactless integrated circuit chip containing a standardised facial image and a degree of cryptographic security to the familiar passport book, preserving all the existing security features. The next phases, probably overlapping in time, include:

- Border Control Inspection systems to take advantage of the features of ePassports
- eVisas using the same type of contactless chip technology
- National eIdentity documents
- Increased biometric content in ePassports or either of the above

This paper focuses on the issue of increased biometric content. We have also published a paper on inspection systems.

Extended Access Control (EAC) has been introduced as the means by which more sensitive biometric content to be added to the next generation of European ePassports will be protected against unauthorised use. Specifically, finger images will need to be protected because, if captured and subsequently abused by 'the bad guys', some unpalatable scenarios could arise.

2 WHAT IS EAC AND WHERE DOES IT FIT?

EAC is a member of the family of security measures introduced by ICAO. EAC, being the most advanced and (currently) being optional, is not yet fully specified. However, a very comprehensive proposal[2] from the German national IT standards body BSI provides most of the detail needed by prospective implementors.

The family of ICAO security measures includes:

- Passive Authentication (PA) – allowing readers to check that the ePassport has been signed by an appropriate issuing authority, i.e. that it is genuine.
- Basic Access Control (BAC) – protecting against reading the passport without the holder's involvement. Without BAC the ePassport contents could potentially be 'skimmed' when the holder least expected it.
- Active Authentication (AA) – protecting the uniqueness and authenticity of the IC chip within the ePassport. This should be used only where BAC is already established.
- Extended Access Control (EAC) – restricting access to certain elements of the ePassport's contents to authorised parties, such as border control, only. This capability will be used to protect fingerprints, iris scans, etc.

Uniquely, the EAC protocol requires authorisation from the ePassport issuer to allow certain specific data groups to be read by specified groups of readers. Without this protection anyone with the necessary technical skills could read the whole passport. When implemented, EAC will have the effect of strengthening all the other security measures because the protocol will not operate stand-alone. EAC-equipped readers will link back to national Public Key Directories (PKD) so Passive Authentication need no longer blindly trust the document signer

[1] International Civil Aviation Organisation www.icao.org which covers, inter alia, aviation safety and security

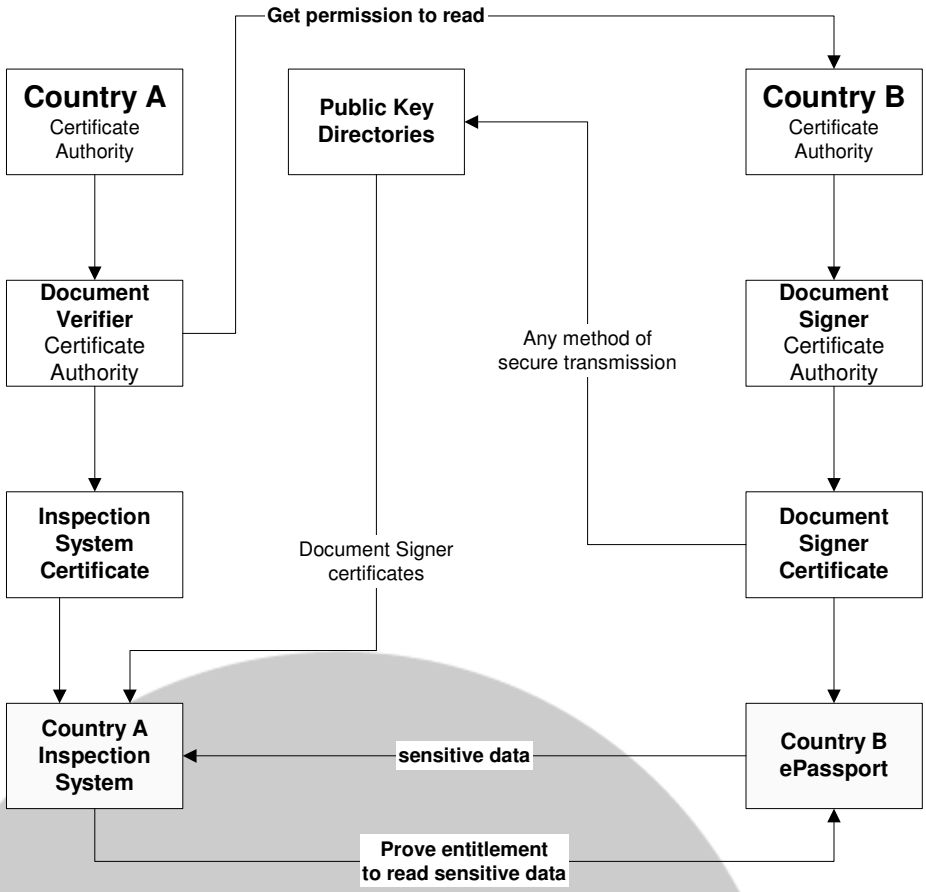
[2] BSI TR-03110 – Technical Guideline: Advanced Security Mechanisms for MRTDs – Extended Access Control v1.0

certificate held within the ePassport. Instead, this certificate can be validated against the country signer certificate in the PKD.

3 HOW DOES EAC WORK?

The diagram shows the workings in a highly simplified form.

Fig. 1



Country A's inspection system is presented with an ePassport issued by country B. A's inspection system wishes to access finger images in the ePassport.

The groundwork for this has been prepared ahead of time. Country B was asked for permission for this type of access and as a result, country A was able to issue an appropriate inspection system certificate. The inspection system first authenticates the ePassport ('Chip Authentication'). A specially-adapted key-agreement[3] protocol is used to enable each end to independently generate the same secret key to secure the subsequent steps. This gives a much greater level of protection than that afforded by Basic Access Control, including resistance to man-in-the-middle attacks.

The ePassport then challenges the inspection system to prove its entitlement to read the sensitive data ('Terminal Authentication'). The inspection system provides a certificate chain back to the aforementioned inspection certificate that represents that entitlement. This is signed using the key from the Chip Authentication stage. When this is all verified the ePassport can release the requested finger images.

[3] A variant of Diffie-Hellmann key agreement described in reference TR-03110

4 WHY IS EAC NOT BEING USED ALREADY?

It should be clear from the above that the infrastructure required for implementation of EAC is non-trivial. The permission-to-read interaction could be done in many possible ways and there is, as yet, no ready-implemented, practical standard for this.

The standards picture for the EAC protocols is not yet complete at a detailed level. As such, it would be risky for issuers to manufacture any EAC-enabled ePassports or for the suppliers of inspection systems to build their solutions just yet.

Many countries are working on their key and certificate management processes and supporting infrastructure. This is non-trivial because of the international scale of the necessary solution. Significant performance challenges are involved in routing current and timely information to inspection stations. These challenges are discussed in our paper on inspection systems.

However, up to now, ensuring that the ePassport production process runs smoothly has been the top priority. Inspection systems have necessarily been on a back burner. A deadline of 2008 has now been set for the issue of EAC-enabled ePassports. The time is right, therefore, to establish the necessary infrastructure for certificate distribution.

5 WHAT IS BEING DONE TO ENABLE THE USE OF EAC?

The custodian of EAC has until recently been the Essen Group[4] consisting of representatives from Germany, Netherlands and the UK. They have worked with the aforementioned proposal from BSI and brought that proposal to an agreed conclusion.

From this point onwards a new gathering with broader European representation known as the Brussels Interoperability Group (BIG) has taken up the EAC mantle. This is the group that will take EAC forward to become an agreed standard with the necessary specifications, probably via ISO.

Inevitably, with a complex proposal such as EAC, the devil is in the detail and there is much detail to be resolved. Nevertheless, it is reasonable to expect that this can proceed smoothly once the initial ePassports move into full production in Q4 2006.

At a review of BIG given at the recent ePassport Interoperability conference in Berlin some challenging comments were heard from the United States (which country does not intend to implement EAC). As was stated in reply, EAC does represent a real challenge but its viability (or otherwise) can be proven within the available timescale.

Technical insight into some of the issues to be resolved is contained in the many papers 'out there', including the aforementioned BSI document (TR-03110 v1.0). A paper from researchers at Columbia University[5] suggesting some further improvements is interesting but somewhat outside the fold at the moment.

A number of organisations have already built proof-of-concept implementations of EAC. More of these implementations are probably needed to underpin the aforementioned standards-making and related test system development activities. Temporal S. is one of the organisations planning work in this area.

[4] Website www.essen-group.org seems to be available in German only.
[5] Preventing Attacks on MRTDs Gaurav and Karger, Columbia University

6 ABOUT TEMPORAL S.

Founded in 2002 and based at Royal Holloway, England – the world-renowned centre of excellence in information security – Temporal S. delivers easy-to-use digital identity (ID) solutions that enable strong IT system security through packaged infrastructure and processes underpinned by Public Key (PK) encryption technology.

Its solutions can be used to address the growing threat of data attack, (internal and external) and provide ID-based mechanisms to enforce, audit and prove compliance with regulatory requirements (e.g. ICAO).

Temporal S. provides specialist support to those organisations producing and issuing ePassports to help them implement ICAO-compliant PKI solutions. Specifically, Temporal S. is focused on the automation and simplification of the set-up and management of PK-enabled solutions - making them easier to use and reducing the service element of their operation.

Temporal S. can provide solutions that address a broad range of ICAO-compliant ePassport requirements, including:

- ePassport interoperability and QA
- ePassport inspection
- ePassport personalisation
- Ease of deployment of ePassport-enabling CAs and PKIs
- Extended Access Control (EAC).

Temporal S. has worked closely with Government and commercial organisations involved in the production and issuance of ePassports. As such, it has developed an extensive understanding of the technical and commercial implications associated with the incorporation of secure digital ID into physical business applications.

For further information contact:

Simon Lofthouse
Temporal S. Limited
enquiries@TemporalS.com

www.TemporalS.com