

43
84

ICAO Specification

Comments on Technical reports

First approach

July 22, 2003

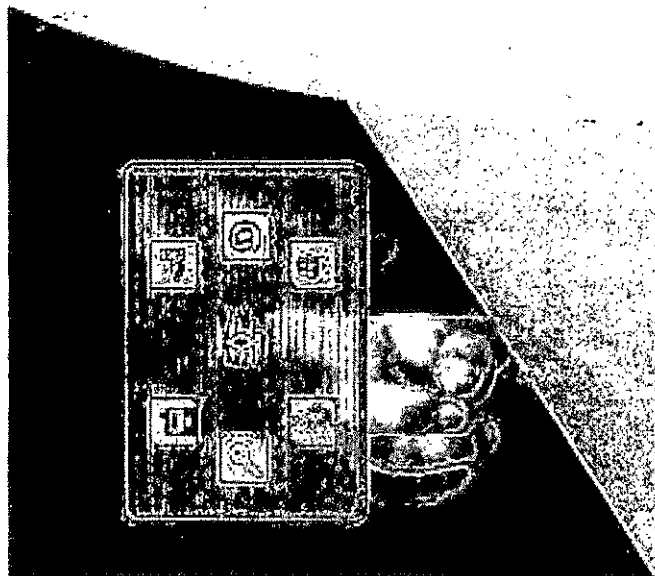
Patrice Plessis ID & Security Dpt

Jean Paul Caruana BDG Contactless Dpt

- Security aspects: General remarks
- Common criteria
- Technical Report on Biometrics deployment
- Privacy
- Fraud
- Set of commands & chip capacity



CONFIDENTIAL



Security aspects: General remarks

- Many pending points impact the product definition & chip capacity. Authentication mechanism is one of these points. Privacy management is a key point in such program. How the fraud detection could be managed to prevent the usurpation of identity, especially with contactless chip? So, it will be important to tackle mutual authentication.
 - ⇒ strong and secure authentication mechanism, access log, ...
- Risk analysis is available for paper version of passport. We don't know if such document exists for an electronic one! Without this document, it's very difficult, in a global point of view, to be sure that the electronic version answers to the threats.

CONFIDENTIAL

GEMPLUS

Common Criteria

- The specifications require high security, tamper-resistance...but nothing is suggest how to verify the acceptance level (CCEAL, laboratory...)
- ⇒ *European laws state that such device needs to get a minimum CC EAL4 certificate, required in many types of applications.*
- ⇒ *The Common Criteria is an international standard (ISO15 408), which is now mandatory for NIST/NSA to protect the information systems and networks that play a role in the United States critical information infrastructure.*
- ⇒ *Fraud reduction : this certificate is an objective validation of the Chip/OS security level. It does not rely on self assessment. It provides the evidence that State owned organizations have tried to attack the device unsuccessfully. Common criteria evaluation provides the customer with a level of confidence over the device. This certificate ensures that the operating system is resistant to a number of attacks.*
- ⇒ *The criteria of an evaluation met prove that the Chip/OS is resistant to:*
 - Confidential data disclosure, Disclosure of application code, keys, PIN, Identity usurpation, Management of JCP ES/application by unauthorized administrators, Use of application by unauthorized user, Data integrity loss, Use of non-valid asset application, keys, PIN, etc.
- **In brief, the evaluation proves that the Chip/OS:**
 - prevents unauthorized operations from applications and/or actors
 - does not contain flaws in design/test
 - ensures a secure loading process of non-aggressive application
 - is resistant to DPA and similar forms of attack

CONFIDENTIAL

GEMPLUS

Biometrics deployment

- Several points are optional. How can it be managed in a global plan between the options really onboard?
- Who should be in charge of the test suite to insure of the minimum requirements?

Example: Mandatory/Optional - ...shall / ...can

P27 "Recommendation ... storage of the image is mandatory, and storage of an associated template be optional at the discretion of the Issuing State. ?

P29 "Recommendation - storage of "optimally-compressed images" is mandatory"


P35 "...chips with cryptographic co-processors on board can use challenge-response protocols to verify the chip has not been removed and placed in a different MFRD. Authenticating users before releasing data from the chip provides confidentiality for the information stored on the chip and it also makes skimming and producing duplicate chips more difficult"

Major impacts on the development and chip selection:

- ⇒ Mechanism may be implemented / which one / set of commands?
- ⇒ how the external environment is informed to manage this mechanism or not?

CONFIDENTIAL

GEMPLUS



Privacy

1/2

- The main goal is to prevent the identity stolen. So external access need to be registered and the user would get the right to check all access (*authorize or not*); that amounts to saying that data need to be exchanged only with trusted terminal (*mutual authentication*).
- An other approach could be the integration of a mechanical button in the contactless layer to release the transmission data, case by case, and under user control.

Privacy

2/2

- The limits of the use of biometrics need to be managed by state drastically (cf Tech. Rep. Biometrics V1.9 ch11 "Biometrics information on a travel document will be captured and used by States, airlines and other authorities and it will become available for uses outside border control (eg banks)
- Biometrics is used for identification in such border control application. If we want to use it in another context, be careful "facial image" is not revocable... (cf P43)

Fraud

1/2

- "Skimming": The specification recommends a distance of 0 to 10cm but we have to precise the maximum characteristics and measure conditions for the system reader.

In fact, it's always possible to "boost" an unauthorized reader to capture data at 20cm or more for example.

⇒ **So, trusted devices/WW key management should be re-examined (not only for skimming threat) cf proposition in tr PKI document.**

CONFIDENTIAL

GEMPLUS

Fraud

2/2

- Cf the recommendations of t.r. PKI and Biometrics documents, the card will contains information's & images signed by state, ICAO and perso manufacturer. There is a major security problem if we put in addition all public keys in the card necessary for the signature verification. In this case it will be possible to create a "right-counterfeited chip" for the electronic part if we don't take precautions; Pb is well known today. *(cf Tech. Rep. Biometrics V1.9 ch11 "The biometrics information should be stored in a way to allow electronic authentication by the simplest possible means commensurate with the security requirement for travel documents. This will involve storing a digital certificate/public key on the document, as it would be impractical to manage worldwide certificate revocation lists")*.

There is an other proposal in the last TR PKI "An alternate and potentially better way to distribute keys associated with specific MRTDs would be to include the public key as well as the DS on the MRTD itself".

CONFIDENTIAL

GEMPLUS

Set of commands and chip capacity 1/2

- There is only a minimum set of commands describes in the specifications.
 - Not enough details on 7816-4 control parameters for the command exchanges or to implement secure mechanism.
 - Data Format available; but details of implementation are missing.
 - In some paragraph it's saying that for integrity reasons we need to write data once time; and few lines under that we have to "*...accommodate future LDS changes and future data additions*".
- ⇒ **This request should be validated with the needs.**
⇒ **Main interrogations on the chip choice due to the biometrics**

CONFIDENTIAL

GEMPLUS

Set of commands and chip capacity 2/2

- ECC is the default algorithm. Precisions need to be brought for implementation. In fact, some keys have several groups of parameters.
 - ⇒ Complementary specifications are necessary for implementation and interoperability.
 - ⇒ we will have to check the vocabulary. Some definitions used, are confusing in different documents. (eg: *authenticity/Integrity code versus certificat chVI*)

UNCLASSIFIED

CONFIDENTIAL

GEMPLUS

UNCLASSIFIED

Contactless physical aspect

- MRTD should mixed different technologie : (Type A Ic/ Tybe B Ic and also 15693 Tags).
 - These mixing should be managed carefully to authorised anticollison and inter-operability.
 - Some features needs to be add to the existing standards to define specifics MRTD constraints. eg: resonance frequency limitation for MRV
 - Test methods (10373-6) is define for a single contactless cards. measurements are define only with one IC in the field. A addendum should be done to define guidelines in case of multiple IC in the field.
 - A specific work group has to study how both contactless type can be mixed and tuning product influence (as 15693 required).
- **MRTD has cryptographic capability.** Noise acceptance has to be define to avoid issue during communication.
- **RF Reader must read TYPE A / TYPE B and 15693**
 - a reader antenna specification (or a set of antennas) could be really helpful to avoid field issue.
 - Power must be managed carefully to avoid issue while proximity device are moved near the antenna.

CONFIDENTIAL

 GEMPLUS

Contacts

Patrice Plessis
patrice.plessis@gemplus.com

Jean Paul Caruana
Jean-paul.caruana@gemplus.com

www.gemplus.com

CONFIDENTIAL

