Should and How CC be used to evaluate RFID based Passports?

TELECOM TECHNOLOGY CENTER

Dr. Albert B. Jeng, Elizabeth Hsu,

and Chia Hung Lin

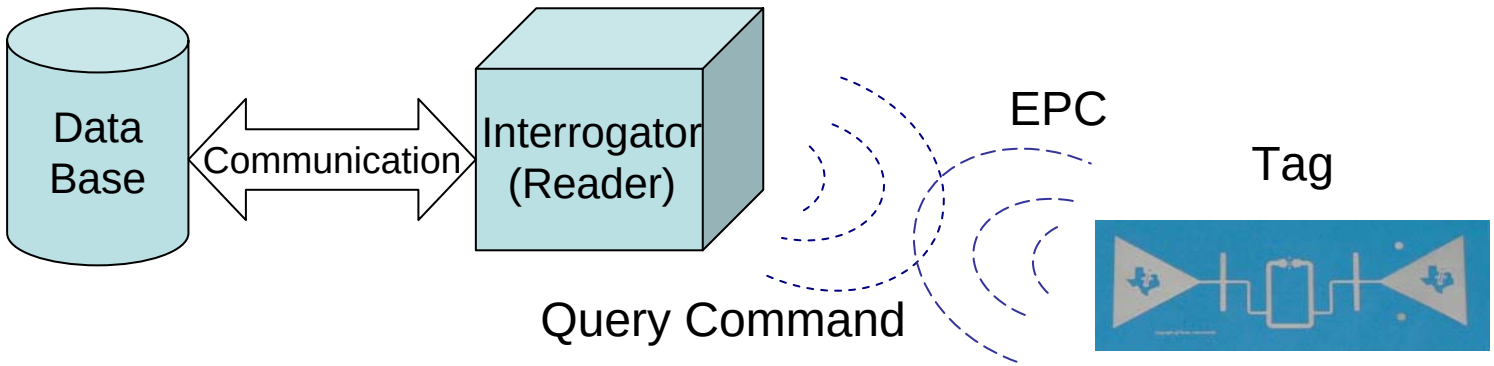
Sponsor: National Communications Commission

Outline

- Overview of the RFID-based passports security
- Should and why CC and/or other standards be used for e-passport evaluation?
- How CC and/or other standards be used for e-passport evaluation?
- Identify the shortfalls for such evaluation
- Proposed Remedy
- Conclusion and Recommendation

RFID Overview

- **A common concern with RFID (Radio Frequency Identification) system is privacy and security risk**



EPC: Electronic Product Code

Overview of Biometric Technology

- **Biometrics are …**
  - Measurable physical characteristics
  - Personal behavioral traits used to recognize the identity, or verify the claimed identity of an individual
- **Examples of Biometric Technologies:**

RFID-based Passports (1)

- " e-Passport" is a Machine Readable Passport (MRP) which is a biometrically-enabled and globally-interoperable passport and conformant to ICAO Doc9303, Part1 Vol.2
  - Doc9303 Part1 Vol.2: e-Passport definition, biometric system, LDS, logical security issues

- e-passport is a combined paper and electronic identity document that uses a combination of RFID and biometrics (facial image photo is required, while fingerprints and iris data are optional) to authenticate the citizenship of travelers.

RFID-based Passports (2)

- The passport's critical information (e.g., biometric data) is stored on a tiny RFID computer chip
  - Biometric data is stored in the passport and sent via the contactless interface to the reader
- Like some smartcards, the e-passport design calls for an embedded contactless chip that is able to hold digital signature data to ensure the integrity of the passport and the biometric data.
- The goal of e-passport is to provide *strong authentication* through documents that unequivocally identify their bearers.
- 36 countries have issued e-passports.

Security Summary of e-Passport

- **e-Passport is a combined system of RFID and biometric technologies**
  - No coherent, integrated security concept for MRTDs has been disclosed either to the general public or to interested experts

    —by P. Gutmann *University of* Auckland
  - [Photo] tampering represents about two-thirds of all passport fraud— by **John Mercer, US State Department Passport Office**
  - RFIDs in passports are a disaster waiting to happen

    • Do you want to broadcast your identity to everyone near you?

    —by Markus Kuhn, Cambridge University
  - Privacy issues never seem to come up in e-passport projects
  - Vulnerability to skimming threats
  - Cloning Threats: copying the signed data stored on the RF-Chip is easily possible in general

e-Passport Security Requirements

- **Data integrity and physical integrity**
  - e-passport must carry a photograph of irrefutable pedigree
  - resistant to tampering or substitution
  - protect e-passports from being forged
- **Data confidentiality**
  - data secrecy affords an important form of protection against forgery and spoofing attacks
  - protecting the secrecy of biometric and biographical data is essential to the integrity of the e-passport
  - protecting e-passport data against unauthorized access
  - protect privacy-sensitive data carried on the passports

Security/Privacy Threats to e-Passport (1)

- **Clandestine scanning**
  - no authenticated or encrypted communications between passports and readers
- **Clandestine tracking**
  - the emission of a unique chip ID on protocol initiation could enable tracking the movements of the passport holder by unauthorized parties.
- **Skimming and cloning**
  - Digital signatures allow the reader to verify that the data came from the correct passport-issuing authority but do not bind the data to a particular passport or chip, so they offer no defense against passport cloning

Security/Privacy Threats to e-Passport (2)

- **Eavesdropping**
  - eavesdropping will be possible on legitimate passport-to-reader communications in a variety of circumstances
- **Biometric data-leakage**
  - Biometric images need to be secret to support authentication in an automated environment with a weak human oversight
- **Cryptographic weaknesses**
  - In an optional mechanism for authenticating and encrypting passport-to-reader communications, once a reader knows the key K, however, there is no mechanism for revoking access

e-Passport Physical Feature

- **Physical MRTD Data**
  - The biographical data on the corresponding page of the passport book
  - Printed data in the MRZ
  - The printed portrait
- **Physical Security Features and Techniques**
  - Substrate materials: UV dull paper, watermark etc.
  - Security Printing: rainbow printing, anti-scan pattern, UV fluorescent ink etc.
  - Protection against copying: electro-photo-printing, thermal transfer printing, laser engraving etc.
- **Placement of the MRTD Chip in MRP**
- **Active shielding on the side(s) of the passport**

e-Passport Logical Feature

- **LDS File System**
  - Smartcard file system for storing Data Elements (personalization and other data
- **Security Mechanism**
  - Implementing the baseline security methods defined Doc. 9303 Part 1 Vol.2 (e.g., PA, BAC, AA, EAC)

Security Function for e-Passport

- **Detection of Forgery/Counterfeit e-Passport**
  - Passive Authentication (PA): Proves that the SOD and LDS are authentic and not changed
  - Active Authentication (AA): Use PKI to prove that the chip has not been substituted
- **Two-level Access Control**
  - Basic Access Control (BAC): Use secure communication channel to prevent eavesdropping
  - Extended Access Control (EAC): Access control to sensitive info. such as finger print data

Summary of ICAO Security Features

Type	Feature Name	Purpose
Mandatory	Passive Authentication Biometric: Photo	Prevent data modification Indentify passport holder
Optional	Active Authentication Basic Access Control Biometric: Fingerprint	Anti-cloning Data confidentiality Identify passport holder

(Source: A. Juels, et al. “Security and privacy issues in e-passports” *IEEE SecureComm*, 2005)

Security Functions vs. Threats

Functions	Threats	Deficiencies
PA	Proves that the contents of the SOD and the LDS are authentic and not changed	Does not prevent an exact copy of chip substitution. Does not prevent unauthorized access Does not prevent skimming
AA	Prevents copying the SOD and proves that it has been read from the authentic chip Proves that the chip has not been substituted	Requires processor-chips (secure cryptographic operation, secure memory etc.) Challenge Semantics
BAC	Prevents skimming and misuse Prevents eavesdropping on the communications between MRTD and inspection system	Does not prevent an exact copy or chip substitution. Requires processor-chips (secure cryptographic operation)
EAC	Prevents unauthorized access to additional biometrics Prevents skimming of additional biometrics	Requires additional key management. Does not prevent an exact copy or chip substitution
Data Encryption	Secures additional biometrics Does not require processor-chips	Requires complex key management Does not prevent an exact copy or chip substitution

(Source: D. Won: “Trend of e-passport in Korea”, TWISC 2008)

Should and why CC be used for e-passport evaluation? (1)

- **Pros:**
  - CC has been applied to access control devices and systems
  - CC has been applied to biometric system
  - CC has been applied to contact-less smartcards
  - CC has been applied to products for digital signature
- **Cons:**
  - CC focuses only on IT product instead of IT system security evaluation
  - CC leaves out the operational environment surrounding the TOE (e.g., “People-based” and physical security)
  - CC addresses *use* of cryptography instead of cryptographic algorithm itself

Should and why CC be used for e-passport evaluation? (2)

- **E-Passport Security Requirements**
- **Mandatory:**
  - Passive Authentication to prevent data modification
  - Biometric: Photo to identify passport holder
  - Physical security to protect forgery/counterfeit/tampering
- **Optional:**
  - Active Authentication for Anti-cloning
  - Basic Access Control to protect data confidentiality
  - Biometric: Fingerprint Identify passport holder
- **e-Passport demands or recommends CC EAL4+/EAL5+ evaluation for the following e-Passport's components**
  - MRTD Chip
  - MRTD Application
  - HSM (Hardware Security Module) for key generation related PKI

Should and why CC be used for e-passport evaluation? (3)

- **Basically, CC and CEM could be used to evaluate most of the "Security Functional Components" and "Security Assurance Components" of the e-Passport security requirements but need to be supplemented in the following requirement areas:**
  - Physical Security
  - Cryptographic Algorithm, PKI and Key Management
  - Operational Security (e.g., administrative, personnel and procedural security)
  - Detection/prevention Cloning /Forgery/Counterfeit

How CC be used for e-passport evaluation (1)

- **Evaluation and conceptual study of new biometric/RFID technologies (in particular RFID, face recognition and cognitive vision)**
- **Development of commonly agreed test and evaluation methodologies with all relevant stakeholders**
  - Develop CC Protection Profiles (PPs) for e-Passport
  - Using CC and CEM to evaluate e-Passport products

How CC be used for e-passport evaluation (2)

- **CC Protection Profiles (PPs) for e-Passport**
  - BSI-PP-0026-2006: MRTD with “ICAO Application” Extended Access Control, Version 1.1, 11 Dec. 2006 (Assurance Package: EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.)
  - BSI-PP-0026-2006: MRTD with “ICAO Application” Extended Access Control, Version 1.1, 7 Sep. 2006
  - BSI-PP-0017-2005 Protection Profile for MRTD with “ICAO Application”, Basic Access Control, Version 1.0, 26 Oct. 2005 (Assurance Package: EAL 4 augmented with ADV_IMP.2 and ALC_DVS.2)
  - BSI-PP-0017-2005 Protection Profile for MRTD with “ICAO Application”, Basic Access Control, Version 1.0, 18 Aug. 2005

How CC be used for e-passport evaluation (3)

- **Biometric Protection Profiles**
  - US (PP_US_BV_BR)
    - ✓ U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments, Version 1.0, 2006-01-12 (Assurance Package: EAL2, augmented with ADV_SPM.1)
  - Germany (BSI-PP-0016)
    - ✓ Common Criteria Protection Profile Biometric Verification Mechanisms, BSI-PP-0016, Version 1.04, 2005-08-17 (Assurance Package: EAL2, augmented with ADV_SPM.1)

CC evaluated e-Passport Products (1)

Deutsches
IT-Sicherheitszertifikat

erteilt vom
Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0445-2007

Security IC with MRTD BAC Application

TCOS Passport Version 1.0 Release 2 / P5CD072V0Q
and TCOS Passport Version 1.0 Release 3 / SLE66CLX641P/m1522-a14

from

T-Systems Enterprise Services GmbH
SSC Testfactory & Security

Common Criteria Arrangement
for components up to EAL4

TCOS Passport Version 2.0, Release 2-BAC/P5CD080V0B

BSI-DSZ-CC-0463-2008

Security IC with MRTD EAC Application

STARCOS 3.3 Passport Edition
Version 1.0

from	Giesecke & Devrient GmbH
PP Conformance:	Machine Readable Travel Document with "ICAO Application", Extended Access Control, BSI-PP-0026
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4

Common Criteria
Arrangement
for components
up to EAL 4

Common Criteria

STARCOS 3.3 Passport Edition Version 1.0

CC evaluated e-Passport Products (2)

PREMIER MINISTRE

Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

CERTIFICAT DCSSI-2008/14

Ce certificat est associé au rapport de certification DCSSI-2008/14

ID-One EPass 64 v2.0 avec EAC ECC

Développeur : Oberthur Technologies / NXP Semiconductors GmbH

Critères Communs version 2.3
(norme internationale ISO/IEC 15408:2005)
EAL4 Augmenté
(ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4)

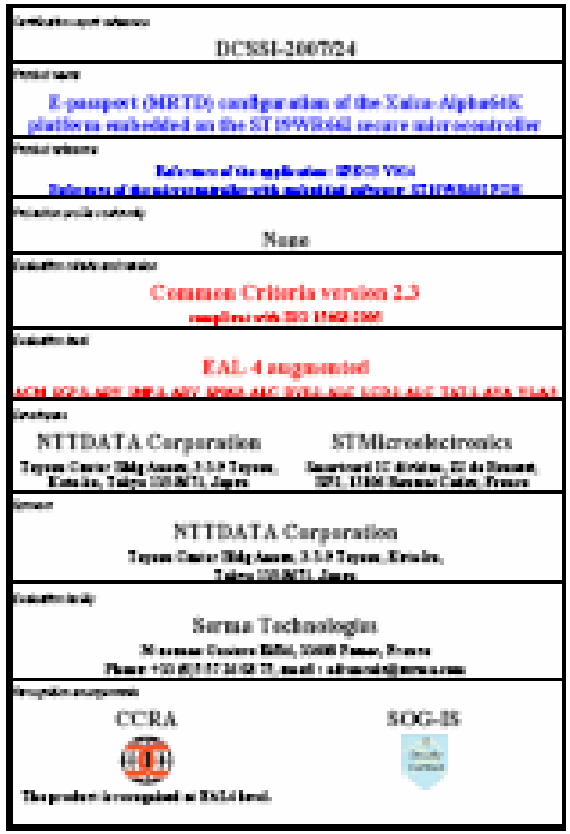
conforme au profil de protection BSI-PP-0026 version 1.2

Commanditaire : Oberthur Technologies
Centre d'évaluation : Serma Technologies

Paris, le 16 mai 2008

Le Directeur central de la sécurité des systèmes d'information
Patrick Pailloux [ORIGINAL SIGNE]

Oberthur Technologies: ID-One EPass 64 v2.0 avec EAC ECC



DCSSI-2007/24

E-passport (MRTD) configuration of the Xaica-Alpha64K platform embedded on the ST19WR66I secure microcontroller

None

Common Criteria version 2.3

EAL 4 augmented

NTTDATA Corporation

STMicroelectronics

NTTDATA Corporation

Serma Technologies

CCRA

SOG-IS

E-passport (MRTD) configuration of the Xaica-Alpha64K platform embedded on the ST19WR66I secure microcontroller

Identify the shortfalls for such evaluation (1)

- **CC relies on the FPT, and FTA to address the measures against forgery threats**
- **CC's handling of the physical protection is both "incomplete" and "insufficient" (too little and too late)**
  - In CC, physical security is generally considered in the Assumption component of the security environment, and in the FPT_PHP, the TSF Physical Protection family
  - The Assumption component addresses physical access control, the FPT_PHP deals with physical tampering and interference.

Identify the shortfalls for such evaluation (2)

- **FIPS140-2 uses Roles, Services and Authentication, Physical Security, and Design Assurance to provide data confidentiality and test the effectiveness of the cryptographic module protection against the forgery attack**
- **In FIPS 140-2, physical security is considered as one of the *eleven* security requirement areas:**
  - protect the integrity of physical “cryptographic module” ,
  - protect all other logic module components (e.g., security kernel or TSF) inside the cryptographic module boundary.

Proposed Remedy

- Supplement CC with FIPS 140-2 to deal with the above drawbacks except operational security
- Use BSI WD Advanced Security Mechanisms for MRTDs – EAC – Tests for Security Implementation, Version 1.0, Jul 2007 as a basis and supplemented with FIPS 140-2 and ISO/IEC 27001 to evaluate overall e-Passport system security

Conclusion and Recommendation (1)

- **CC has intrinsic weakness and existing e-Passport PPs have drawbacks in the following security evaluation:**
  - Physical Security
  - Cryptographic Algorithm, PKI and Key Management
  - Operational Security (e.g., administrative, personnel and procedural security)
  - Detection/prevention Cloning / Forgery /Counterfeit
- **e-Passport had been evaluated only in a piecemeal manner in component level (e.g., MRTD Chip, MRTD Application, HSM)**

Conclusion and Recommendation (2)

- Need to establish a comprehensive security evaluation of e-Passport system similar to US GSA FIPS 201 Evaluation Program (EP) to evaluate the security and interoperability of e-Passport
- A more fundamental fix to e-Passport security is to develop a clear threat model and show e-Passport has a coherent, integrated security solution

Reference (1/2)

[1] A. Juels, D. Molnar, and D. Wagner. Security and privacy issues in e-passports. IEEE SecureComm, 2005.

[2] P. Gutmann, Why Biometrics and RFID are not a Panacea, Univ.of Auckland, New Zealand 2007

[3] D. Won. Trend of e-passport in Korea. TWISC, 2008.

[4] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 2, Sept 2007.

[5] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 3.1, Revision 2, Sept 2007.

[6] Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 2, Sept 2007.

[7] BSI WD Advanced Security Mechanisms for MRTDs – EAC – Tests for Security Implementation, Version 1.0, Jul 2007

[8] ICAO Doc 9303 MRTD Part 1 MRP, 6th Edition 2006

Reference (2/2)

[9] ICAO Supplement to Doc_9303_Part 1_6th Edition 2006 (Final: release 5, Feb 2007)

[10] US (PP_US_BV_BR) U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments, Version 1.0, 2006-01-12

[11] Germany (BSI-PP-0016) Common Criteria Protection Profile Biometric Verification Mechanisms, BSI-PP-0016, Version 1.04, 2005-08-17

[12] BSI-PP-0026-2006: MRTD with "ICAO Application" Extended Access Control, Version 1.1, 11 Dec. 2006

[13] BSI-PP-0017-2005 Protection Profile for MRTD with "ICAO Application", Basic Access Control, Version 1.0, 26 Oct. 2005

[14] NIST and CSE, *Security Requirements for Cryptographic Modules*, issued at May 25, 2001.

[15] GSA FIPS 201 EP: (http://csrc.nist.gov/groups/SNS/piv/npivp/index.html), and the GSA FIPS 201 EP website (http://fips201ep.cio.gov)

[16] e-Passport Security and Testing Dr Pravir Chawdhry, JRC, EC, Ispra, Italy, December 12, 2007

Thanks for Your Attention !

albertjeng@hotmail.com, bethhsu@ttc.org.tw, chlin@ttc.org.tw

http://www.ttc.org.tw