



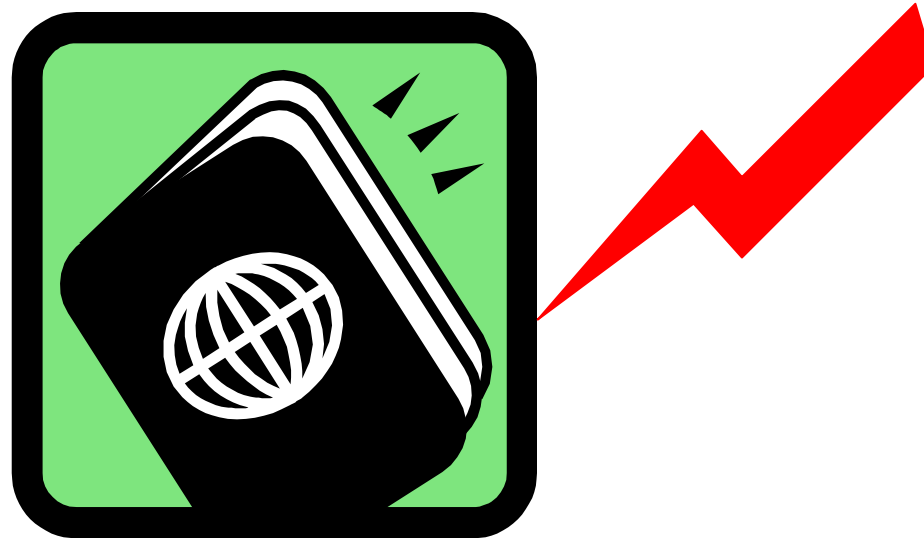
Thomas J. Watson Research Center

ICAO RFI Response: High-Assurance Smart Card Operating System for Electronic Visas

Paul A. Karger
karger@watson.ibm.com

The Challenge We are Addressing

How does one country maintain the integrity of an official *electronic* document that **other** countries write in,
e.g. *electronic* visa stamps in an *electronic* passport?



Tomorrow's proposed solutions

- Conservative solution
 - maintain today's system of paper stamps / stickers in passports (don't let foreign countries write on the chip)
 - maintain separate machine readable work permit cards
- Possible advanced solutions
 - paper stamps / stickers in passports with biometrics in central database
 - e-visa / residency smart cards containing biometric data
 - e-visa / residency smart cards + paper stamps / stickers in passports
 - add more chips in the e-passport, but these cause collisions at the readers – cannot resolve which chip is which

Our proposed solution

A high assurance operating system in a single chip that

- permits authorized writes
- protects itself from unauthorized writes
- access controls and software can be safely updated in the field
- is a possible candidate for second-generation MRTDs

Why aren't today's smart cards strong enough to share write access among nations and dynamic coalitions?

Not yet good enough (hardware and standards)

■ Hardware

- Software must be aware of and compensate for limited hardware defenses, which are limited by cost, power consumption, physical dimensions, weight
- Attackers can mount offline, slow, sophisticated attacks on one stolen or legitimately obtained device
- New ways to intentionally or inadvertently leak data are enabled through chip emanations (e.g. power, radio frequency)

■ Standards

- Smart cards must follow application interoperability standards, even if that means divulging sensitive information to hostile readers
- Authentication is left up to the application. In this environment, one application should not trust another application or its users.

Not yet good enough (software)

- Software and software development
 - Existing system evaluated at EAL4+ are not very strong.
- No developer has (yet) reached EAL6 or EAL7 (true high assurance)
 - The rigorous security required for such applications must be designed in from the very start
 - Systems have achieved ITSEC E6 or Orange Book A1
- National agreements are dynamic.
 - Alliances between countries come and go
Current software supports prearranged access controls.

What is high assurance? How can it help?

- Provides a level of security sufficient to resist sophisticated, well-motivated, and well-funded attackers
- Built to very high standards
 - Common Criteria: EAL6 or EAL7
 - Orange Book: B3 or A1
 - ITSEC: E5 or E6
- The process of third-party evaluation motivates developers not to take shortcuts

High-Assurance Smart Card Operating System

- A better solution would be to allow each country to write its own visa (or residence permit) onto the single e-passport chip
- IBM Research Division has been developing exactly that solution – not a product, just a research project
 - Caernarvon High-Assurance Smart Card Operating System
 - Designed to be evaluated at Common Criteria EAL 7
 - Assumes that applications may be mutually hostile and provides inter-application protection AND controlled sharing between applications
 - We have a working alpha-test-level prototype

Caernarvon Castle – North Wales



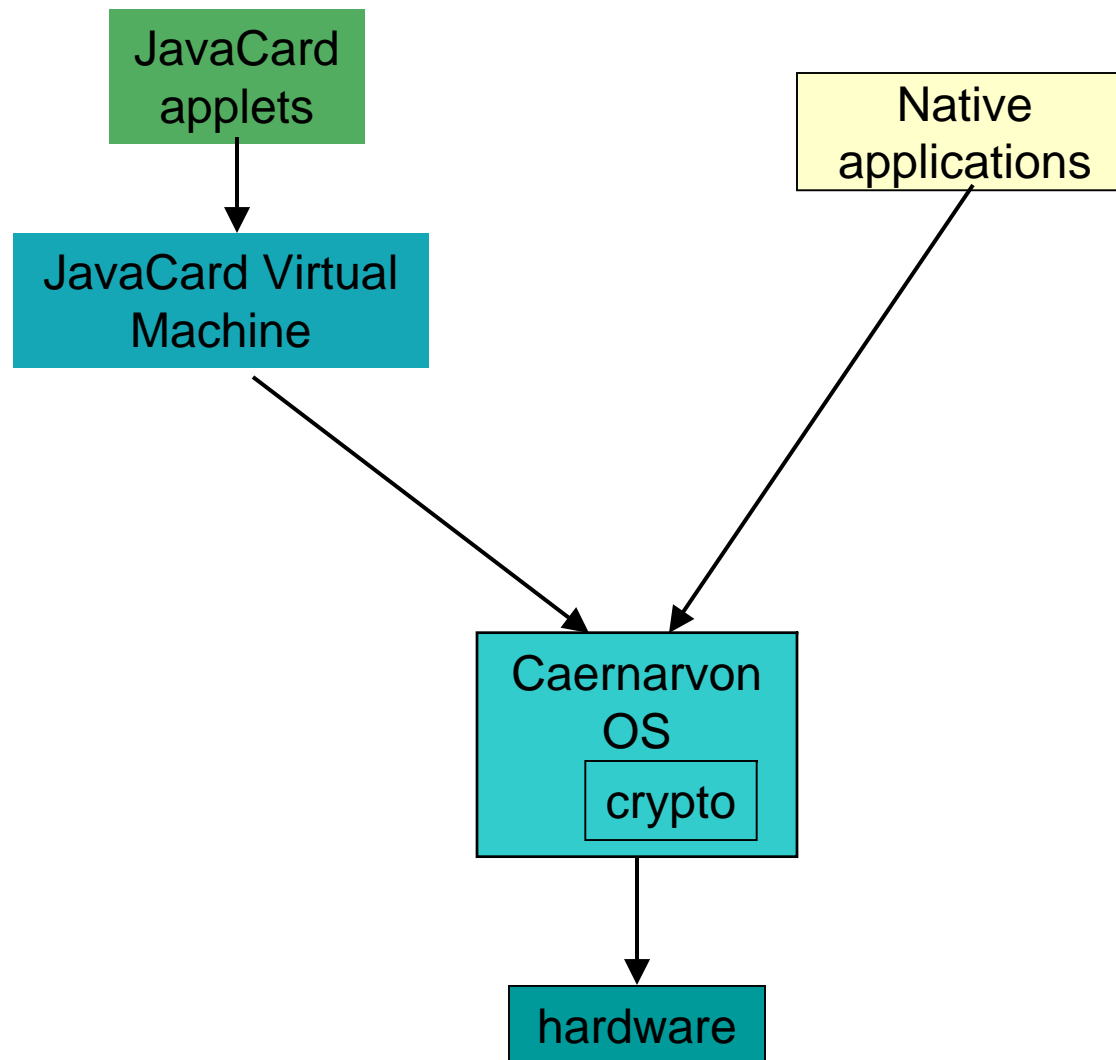
Need for Stronger Hardware Protection

- Most smart card chips provide no hardware security
 - No separate user/system modes
 - No memory protection
 - All code within the card can access anything within the card
- Some newer smart card chips have protection
 - User/supervisor modes
 - Memory protection

Caernarvon Smart Card Operating System

- Requires and uses
 - supervisor/user mode separation
 - full memory protection and addressing virtualization
- To enforce
 - Protection of the OS and persistent storage from applications
 - Protection of one application from another
- Currently runs on Philips SmartXA2 16-bit smart card chip
- Other Candidates
 - Philips HiPerSmart
 - Infineon SLE88
 - others

Structure of a Caernarvon Smart Card



Countries to be Used in Examples

- With apologies to Gilbert and Sullivan
- Passport issuing country – Utopia, Ltd.
- Visa issuing country – Duchy of Pfennig Half-Pfennig
- Enemy country – Barataria

Access Controls

- Mandatory Access Controls (MAC)
 - Access control is controlled by an administrator, rather than the owner of the data or an untrusted application program
 - Can be mathematically proven to resist Trojan horse and virus attacks
 - Originally developed for military applications
 - Caernarvon model significantly extends MAC for commercial uses

Caernarvon MAC is multi-organizational

- Traditional MAC comes from the Defense world, where there is a single organization – the Department of Defense
 - Inadequate for commercial use, because there may be thousands of organizations, each with its own authority
 - Inadequate for multi-national military alliances – would Utopia, Ltd. trust Baratania to issue Utopia, Ltd. security clearances, or vice versa?
 - No single certificate authority hierarchy can meet these needs!

Caernarvon Universal Access Classes

- A traditional access class consists of a sensitivity level and a set of categories

Level	Category 1	...	Category N
-------	------------	-----	------------

- An organizational access class (OAC) is a traditional access class with an organization ID – level and category meanings are per organization

Organization ID	Level	Category 1	...	Category P
Utopia, Ltd.	Sensitive	Passport Data	...	Driver's License Data

- A universal access class (UAC) is a set of OACs.

OAC 1	...	OAC Q
-------	-----	-------

- These are all secrecy access classes – integrity (for card software) would look the same

Universal Access Classes for Electronic Visas

- Each country is an organization
- Passport holder visits consulate to get a visa
- Consulate contacts smart card to download visa
 - Uses special protocol to coordinate with passport issuing country for approval to download the visa
 - Passport issuer has control over whether a visa is downloaded, but it has NO control over the content
 - All countries' data are protected against tampering or unauthorized access by other countries
 - Biometrics can be shared if and only if the passport issuer agrees
 - Separate visa cards are still an option

Data Structures on the Chip

UAC: Utopia, Ltd.

Private Data of
Passport Issuer
only

UAC: Pfennig Half-Pfennig

Private Data of
Visa Issuer

UAC: Utopia, Ltd. +
Pfennig Half-Pfennig

Shared Biometric
Data

Immigration Scenario

UAC: Utopia, Ltd.

Private Data of
Passport Issuer
only

UAC: Pfennig Half-Pfennig

Private Data of
Visa Issuer

No Access

UAC: Utopia, Ltd. +
Pfennig Half-Pfennig

Shared Biometric
Data

Read-only
via guard
process

Read-write

Pfennig Half-Pfennig
Immigration Officer
External Reader

```
graph TD; UAC1[UAC: Utopia, Ltd.] -- "No Access" --> Reader([Pfennig Half-Pfennig Immigration Officer External Reader]); Reader -- "Read-only via guard process" --> UAC2[UAC: Utopia, Ltd. + Pfennig Half-Pfennig]; Reader -- "Read-write" --> UAC3[UAC: Pfennig Half-Pfennig];
```

Attacker Scenario

UAC: Utopia, Ltd.

Private Data of
Passport Issuer
only

UAC: Pfennig Half-Pfennig

Private Data of
Visa Issuer

UAC: Utopia, Ltd. +
Pfennig Half-Pfennig

Shared Biometric
Data

No Access

No Access

No Access

Barataria
Attacker
External Reader

How is Access Control Enforced

- Caernarvon authentication protocol provides cryptographic evidence of the access classes to which any given external reader is authorized
- Caernarvon operating system can then make access control decisions, based on that cryptographic authentication

Where did the countries come from?

- Utopia, Ltd.
 - from **Utopia, Ltd.**
 - incorporated its government as a limited liability company
- The Duchy of Pfennig Half-Pfennig
 - from **The Grand Duke**
 - has had a coup d'état by a troop of actors from a musical comedy
- Barataria
 - from **The Gondoliers**
 - infant heir to throne smuggled out to be a Venetian gondolier

References

- Schellhorn, G., W. Reif, A. Schairer, P. Karger, V. Austel, and D. Toll. *Verification of a Formal Security Model for Multiapplicative Smart Cards*. in **6th European Symposium on Research in Computer Security (ESORICS 2000)**. 4-6 October 2000, Toulouse, France: Lecture Notes in Computer Science Vol. 1895. Springer-Verlag. p. 17-36.
- Karger, P.A., V.R. Austel, and D.C. Toll. *Using Mandatory Secrecy and Integrity for Business to Business Applications on Mobile Devices*. in **Workshop on Innovations in Strong Access Control**. 25-27 September 2000, Naval Postgraduate School, Monterey, CA: published on CD-ROM. URL: <http://www.acsac.org/sac-tac/wisac00/wed0830.karger.pdf>
- Karger, P.A., *Multi-Organizational Mandatory Access Controls for Commercial Applications*, RC 21673 (97655), 22 February 2000, IBM Research Division, Thomas J. Watson Research Center: Yorktown Heights, NY. URL: <http://domino.watson.ibm.com/library/CyberDig.nsf/home>