The development of the common transport smart card coming up to the standard of each Asian economies

Technical Summary of Method 2 :

Multi Smart Card with selector software technology

Infineon Technologies Japan

AIM IM CC

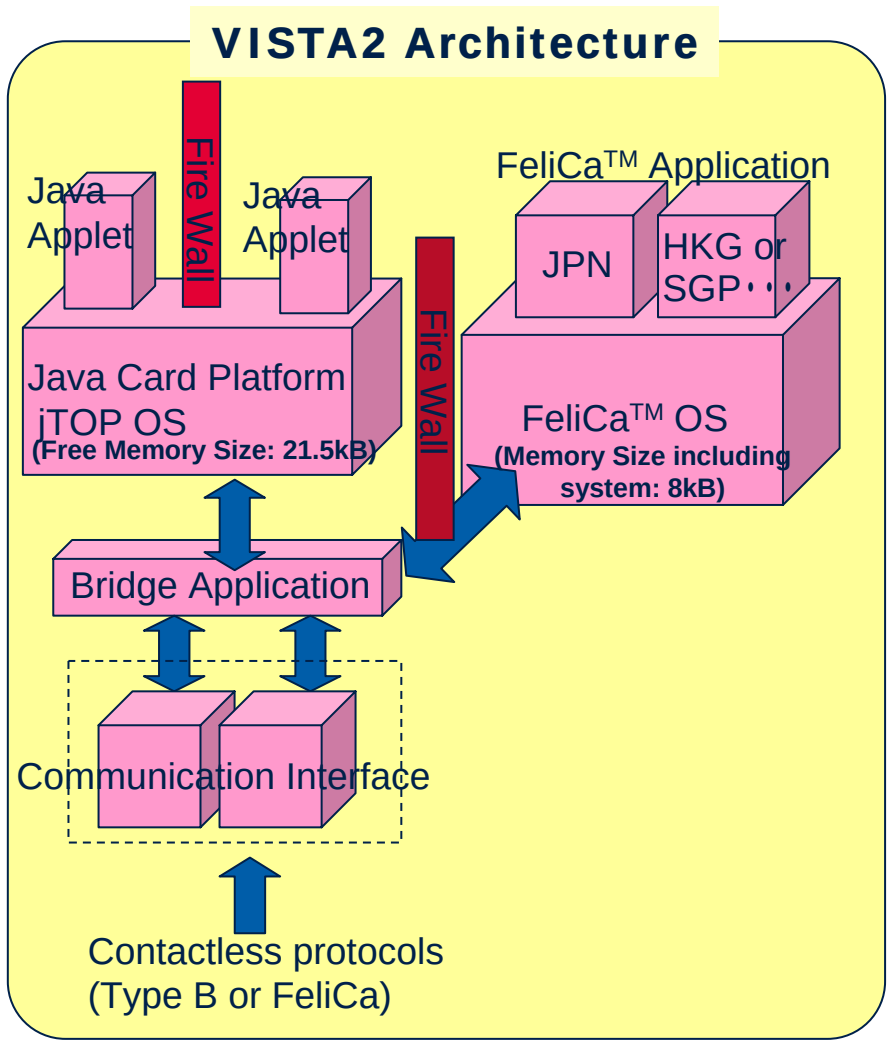
Mayumi Inada

Never stop thinking

Realization method to promote the multi application smart card with selector software technology

“VISTA2” card realized multi-application on multi-OS.

- Fundamental view of architecture
  - Java Card OS and FeliCa OS are on “SLE66CLX320PS” chip, which can support both Type-B & FeliCa interface.
  - Each OS and applications are separated by HW supported “Fire Wall”.
  - FeliCa OS can support up to two transport applications. (Japan, Octopus in Hong Kong and Ez-Link in Singapore, etc.)
  - Java Card OS can support several applications, including transport on Type-B, depending on applet size.
  - Bridge application, which resides between communication interface and OSs, will control the access.
- Workability & Interoperability will be tested.



Security management of demonstration test using selector software technology

>IC chips to be used

The IC chip, SLE66CLX320PS, manufactured by Infineon Technologies AG will be used. The security of this chip is proved by getting Common Criteria EAL5+ issued by BSI*.

Japanese card manufacture will embed this chip into the card under the secure environment.

(EMV certification for JAVA Card OS related part is planned by SONY.)

>Security in the card

In the card, firewalls are constructed between FeliCa OS and JAVA OS, and in between JAVA applets as shown next page. It is not possible to make read nor write access the other area.

>Card handling at the demonstration test

(1) Only the authorized internal staffs can handle the cards. And the cards will not be distributed to the public and will be stored under the secure environment by limiting and clarifying the authorized access.

(2) The cards will be transported (to the another company) by internal staffs.

(3) The limited number of cards will be manufactured. (200 cards will be planned.)

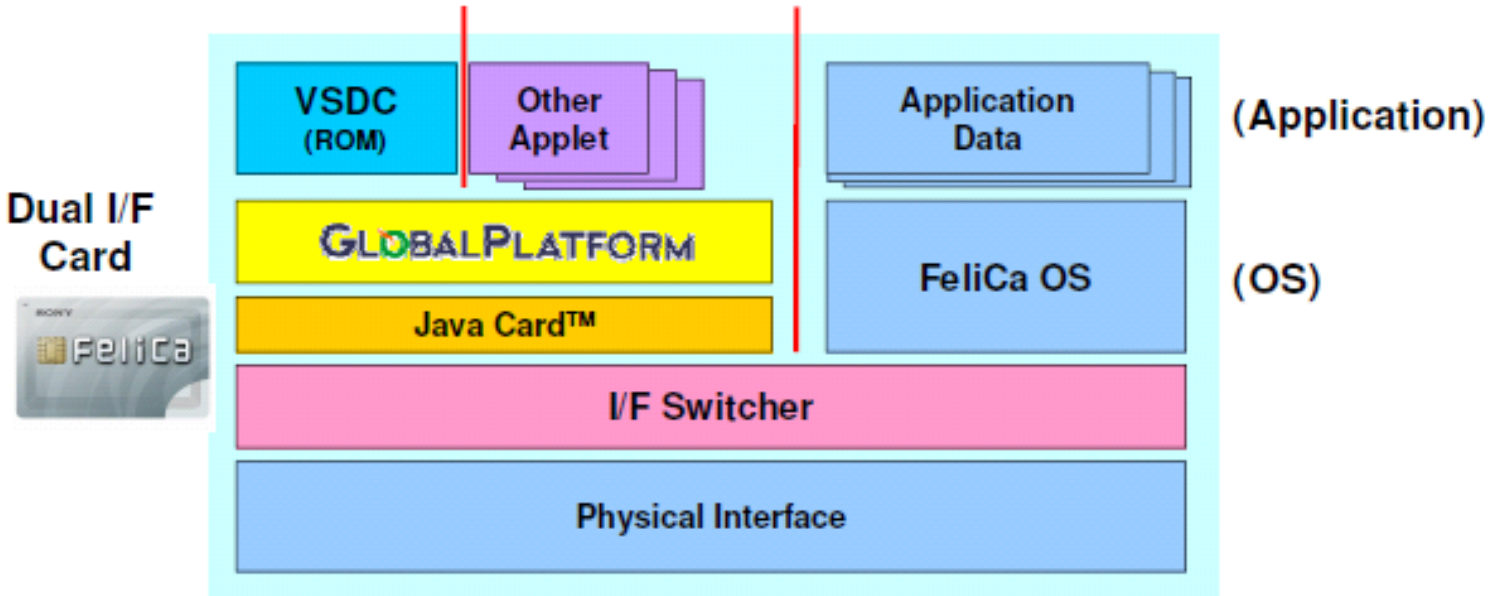
(4) All cards will be collected after the demonstration test and certainly disposed.

*BSI : Bundesamt fur Sicherheit in der Informationstechnik

Internal Software Structure

FeliCa

- Firewall among applications



Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0339-2005

Infineon Smart Card IC (Security Controller) SLE66CLX320PS / m1554b21 and SLE66CLX160PS / m1525b21 both with RSA2048 V1.3 and specific IC Dedicated Software

from

Infineon Technologies AG

The IT products identified in this certificate have been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0* extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

PP Conformance:	**Protection Profile BSI-PP-0002-2001**
Functionality:	**BSI-PP-0002-2001 conformant plus product specific extensions Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant EAL5 augmented by:** ALC_DVS.2 (Life cycle support - Sufficiency of security measures), AVA_MSU.3 (Vulnerability assessment - Analysis and testing for insecure states), AVA_VLA.4 (Vulnerability assessment - Highly resistant)

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 12. December 2005
The President of the Federal Office
for Information Security

Common Criteria