A2-02

Application of the Common Criteria to a Terminal for Banking Services

Yukio Izumi

Mitsubishi Electric Corporation

Atsuko Ogasawara* / Syunsuke Yamamoto* / Tsutomu Morigaki* / Keiki Yamada**

*** Mitsubishi Electric Information Systems Corporation**

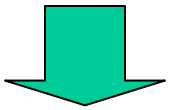
**** Mitsubishi Electric Corporation**

Outline

- What is CBB?
- Scope of the TOE
- TOE development and evaluation
  - ST development
  - Development of other deliverables
  - Evaluation framework
- Conclusion

What is CBB?

- A dedicated terminal for banking services, "CBB terminal", is installed in convenience stores
- Customer can take the following banking services (domestic service only) by using a CBB terminal, without visiting a bank branch:
  - Request for address change
  - Request for automatic withdrawal of utilities payments
  - Request for seal registration change request, etc
- Customer can not withdraw cash from a CBB terminal (ATM≠CBB terminal)



In CBB, the customer is authenticated by his/her Personal Identification Number (PIN)

The CBB terminal

Operation panel with polarized light filter

Bank card insertion slot

Receipt printer

Insertion slot for application form (with envelope)

Physical locks

CBB Terminal for The Bank of Tokyo-Mitsubishi, Ltd.

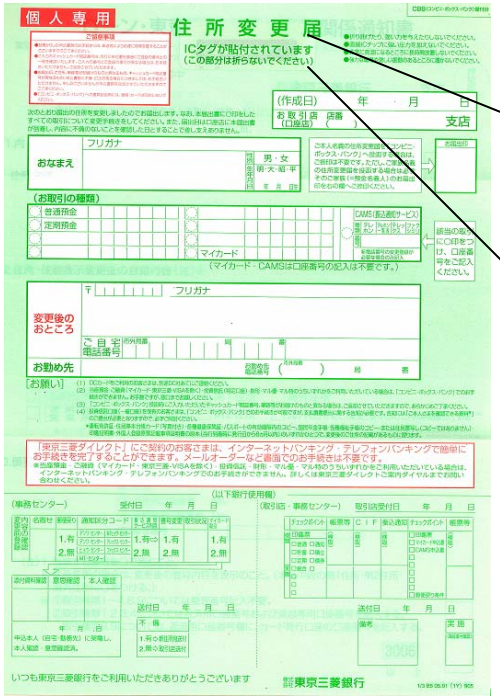
Height of 31.5 inches (80 cm)

How to use CBB

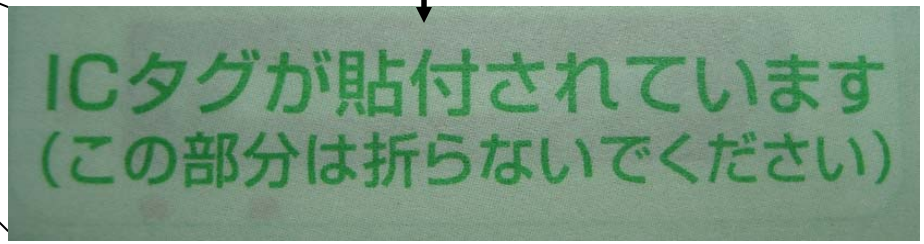
Customer

- Fill out the CBB application form with RFID

e.g. Address change request form



Overleaf

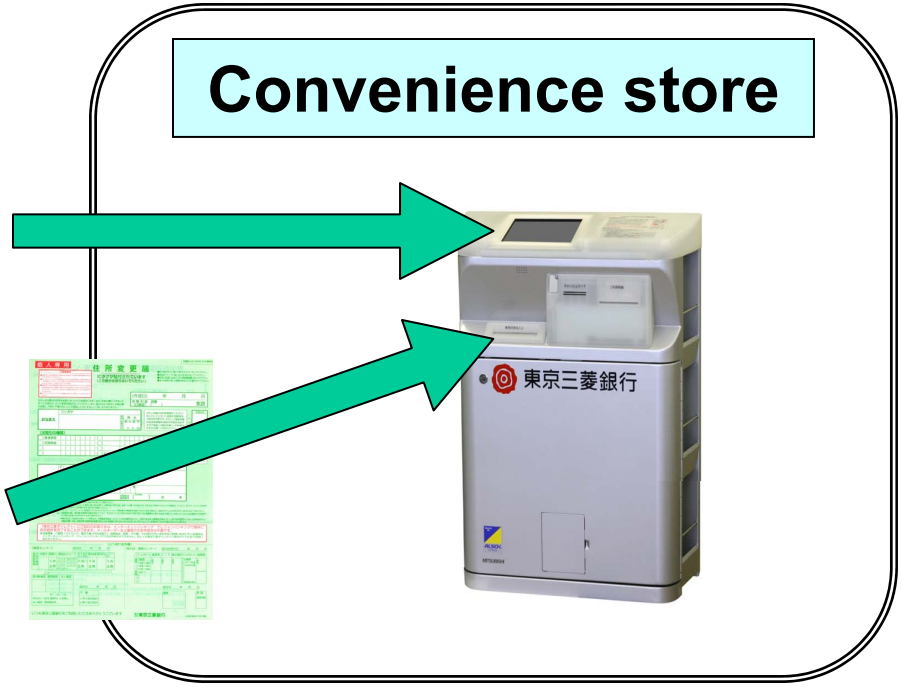


RFID is attached here.
(Please do not fold this part.)

How to use the CBB

Customer

- Choose the service and enter the PIN at the CBB terminal
- Insert the envelope containing the application form into the CBB terminal



CBB terminal

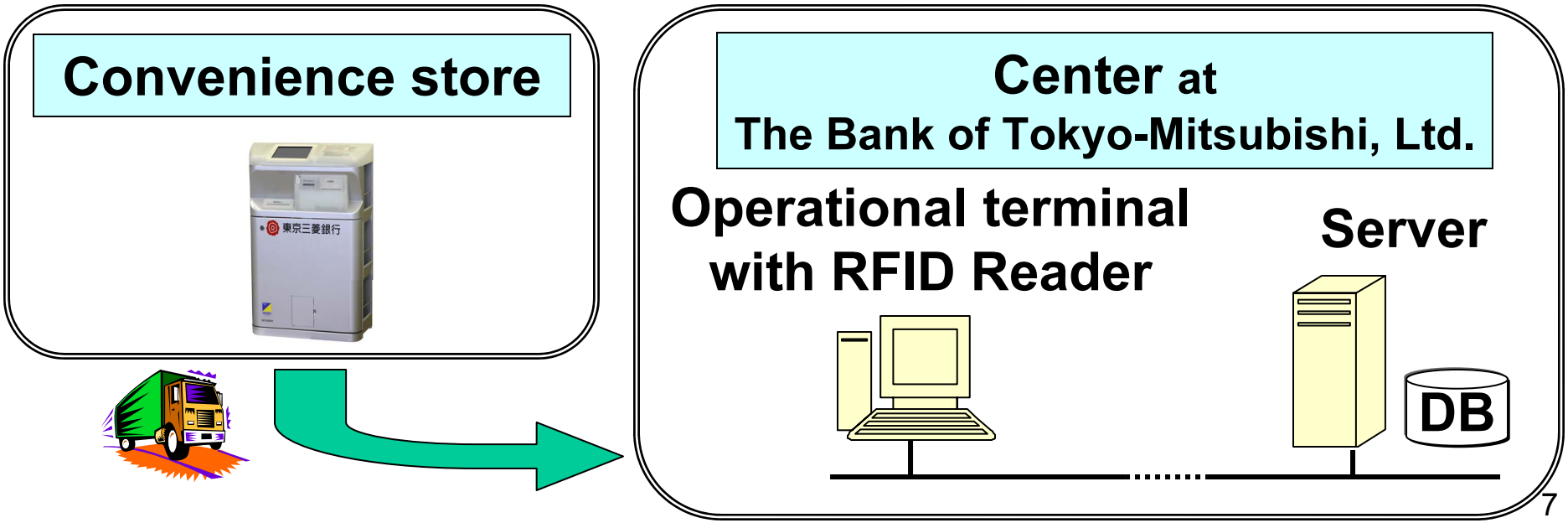
- Record the PIN and other information on RFID

Distributor

- Deliver the application form from the convenience store to the center

Center

- Check the PIN
- Accept and process the request of the services

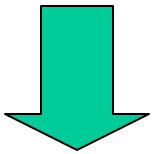


Asset in CBB

The PIN of a customer is important information in the conventional banking system.

In the case of CBB, the PIN is

- **used as authentication information**
- **recorded in an RFID at the convenience store**



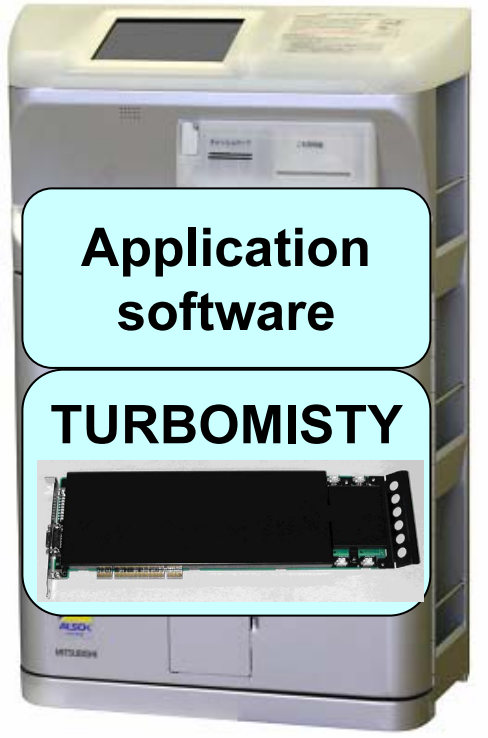
The PIN has to be kept confidential in the CBB, especially at the CBB terminal.

The scope of TOE

The security critical component = TOE

“ CBB business application unit ”

- **Application software**
- **A tamper-resistant security hardware board “TURBOMISTY”**



- **Encryption function**

  Cipher the PIN before recording RFID

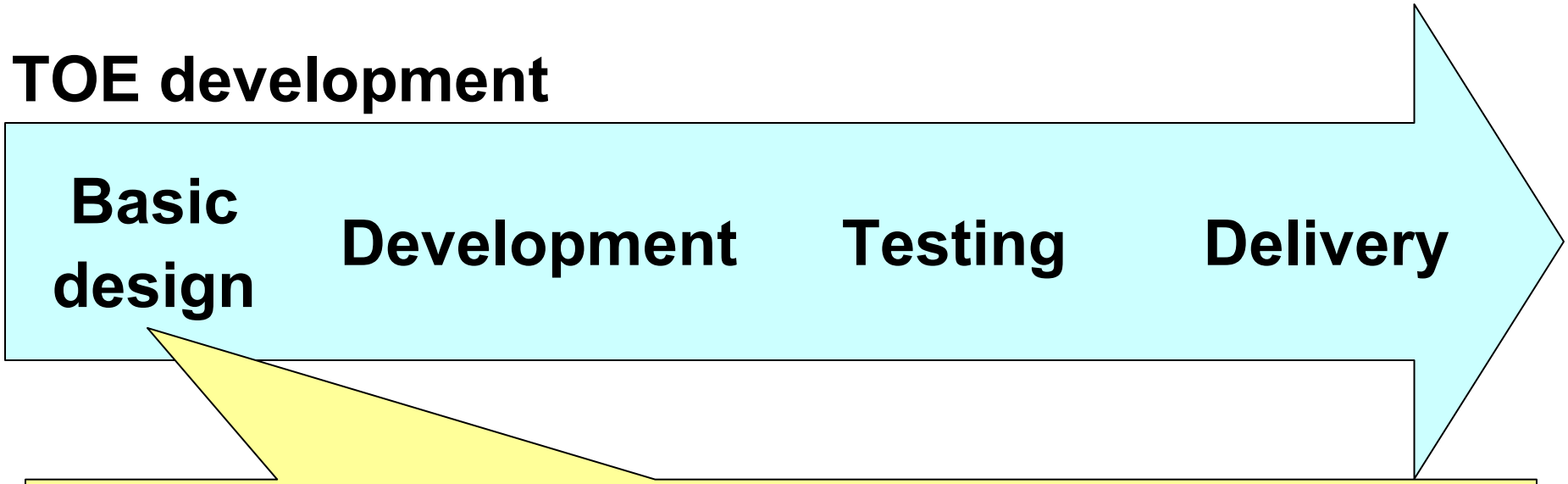
- **Management function**

  Update the encryption key

“TURBOMISTY” is manufactured by Mitsubishi Electric Information Systems Corp.

Early stages of the design

TOE development



- Developing the ST
- Studying the specifications of cryptographic operation and encryption key management in entire CBB
- Surveying the necessary deliverables for CC evaluation

TOE Environment

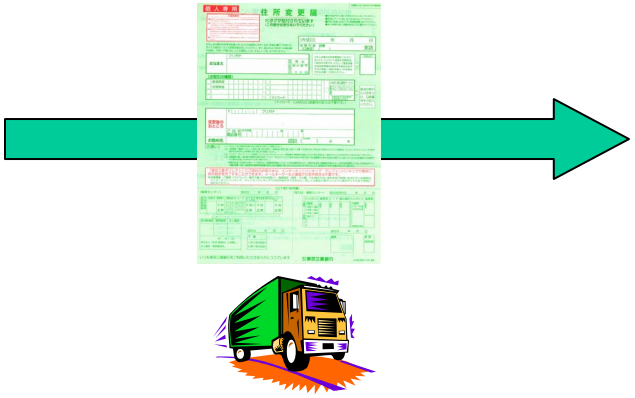
Convenience store

Peeping the PIN

Management of physical keys

Maintenance engineer

Disclosure of the customer's PIN



Management of the PIN for maintenance

Security Objectives for the TOE and Security Functional Requirements

O.PROTECT_INFO

Prevent disclosure of the PIN

→ **FCS_COP.1(M), FCS_COP.1(R), FMT_MSA.2, …**

O.MANAGE

Provide the function for the maintenance work to the authorized maintenance engineer

→ **FIA_AFL.1, FIA_UAU.1, FMT_MTD.1, FMT_SMF.1, …**

The TOE Security Functions

SF.CRYPT

- Cipher the PIN using encryption algorithm “MISTY1” before recording it
- To obtain the MISTY Key, decrypt the ciphered key data using “RSA private key” in “TURBOMISTY”
- Compare the check data in the header of the ciphered key data with one in the decrypted key data

“MISTY1” was developed by Mitsubishi Electric Corp. and was adopted in ISO/IEC 18033.

The TOE Security Functions

SF.MANAGE

- Authenticate the maintenance engineer
- After several authentication failures, deny the maintenance PIN input for 5 minutes
- Allow updating of key data by authorised maintenance engineer only

Security Assurance Requirements

From the technical viewpoint

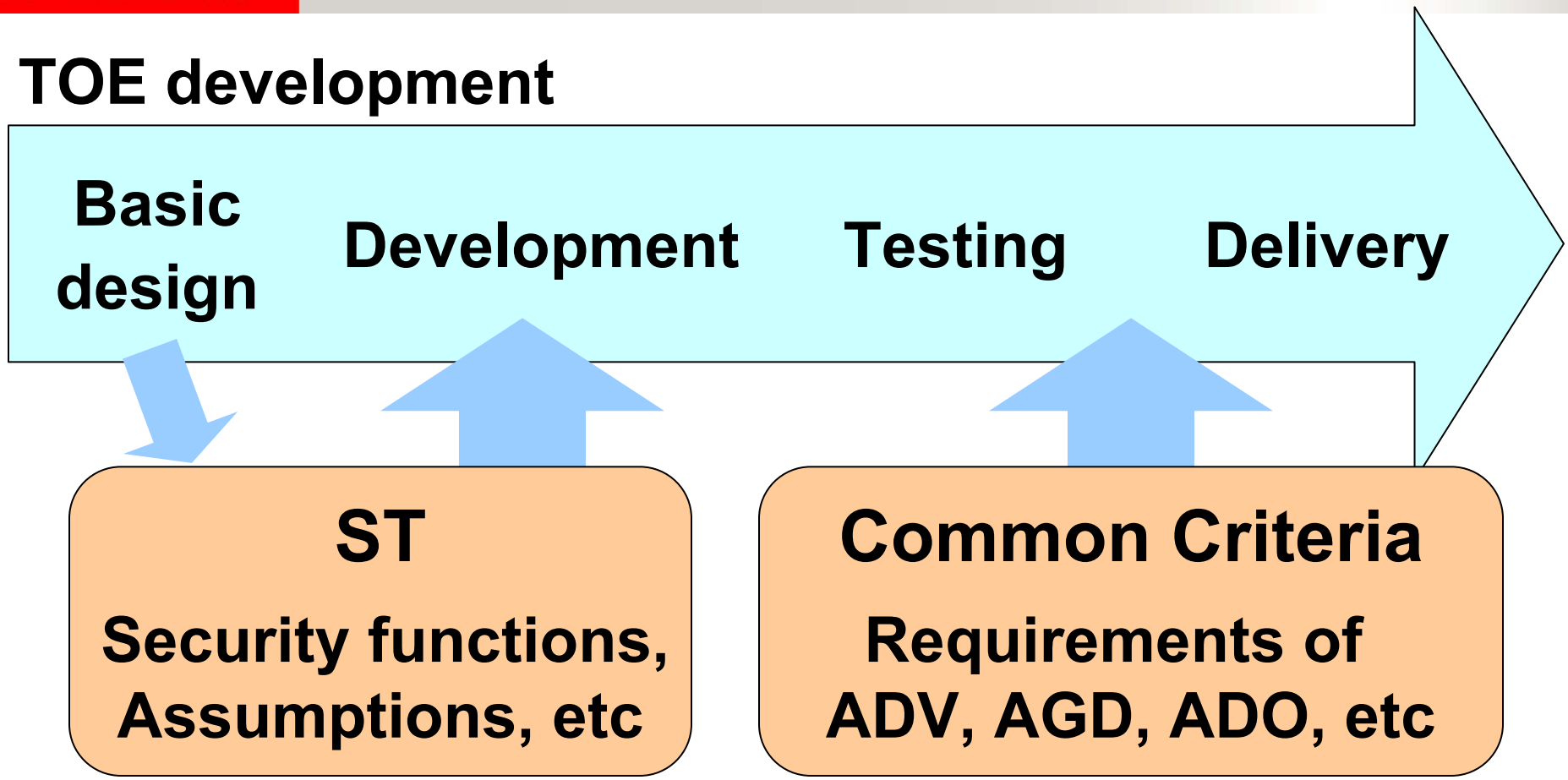
- The CBB terminal is locked physically
- Only Authorized person have access to the TOE
- Only a limited interface is available to the customer (only the operation panel)
- Cash is not handled in the CBB terminal

From the business viewpoint

- Evaluation cost and term
- Release timing (Launch of the CBB services)

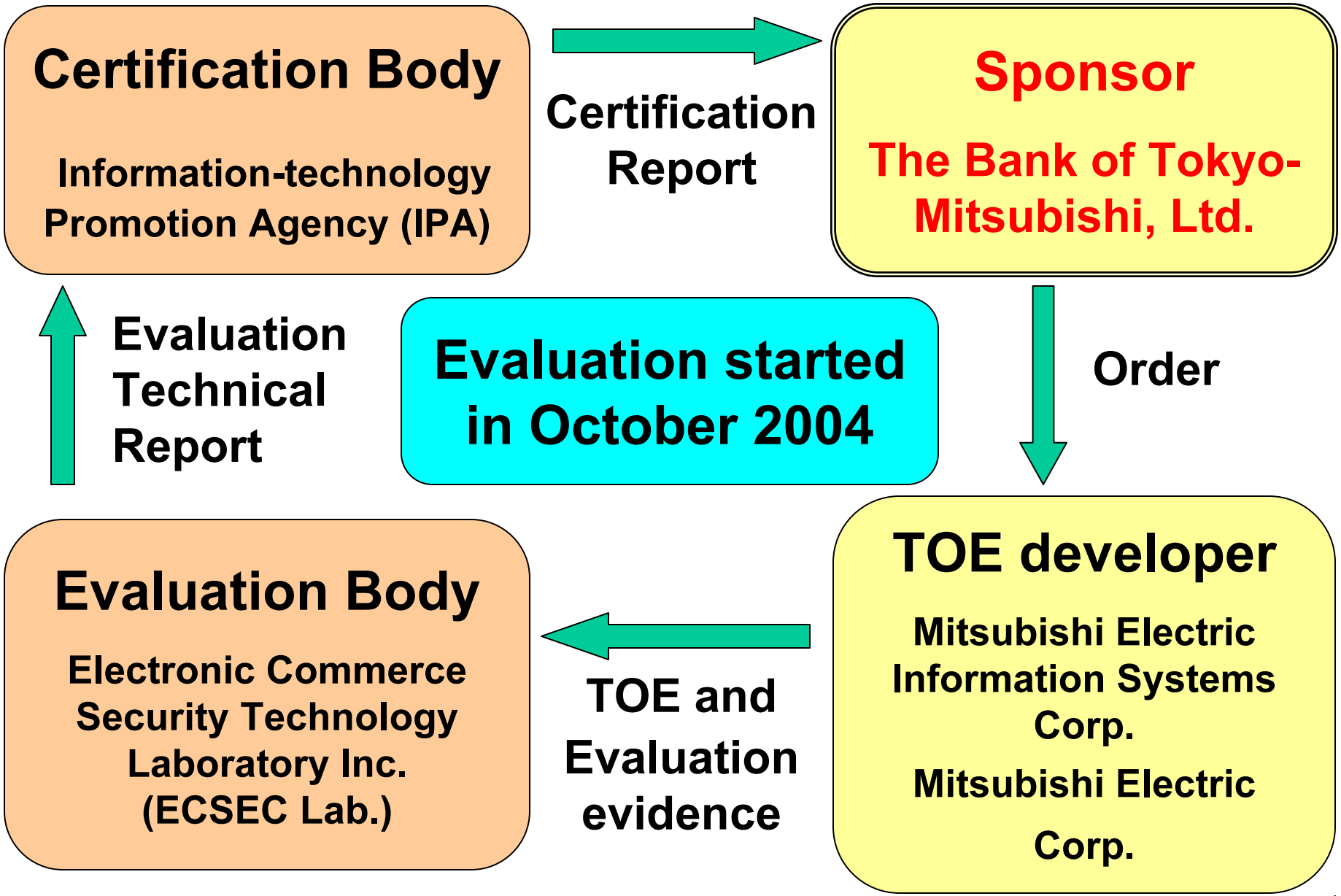
→ **EAL2**

Development of other deliverables



- Develop the TOE based on ST
- Survey and correct some procedures
- Develop the evaluation deliverables in parallel with the real TOE development

Evaluation Framework



Finally…

- This evaluation project was completed in February 2005.
- TOE was first certified in the financial field of Japan in March 2005.
- The time taken for certification was about 5 months.
- The sponsor gave an announcement to the press and launched the services.

Conclusion

In this case, planning the CC from the initial design stage was effective for achieving the development and the evaluation concurrently within a short term.

In the future, I want to examine:

- **Efficient application to other security products**

Thank you!

Yukio IZUMI

izu@isl.melco.co.jp