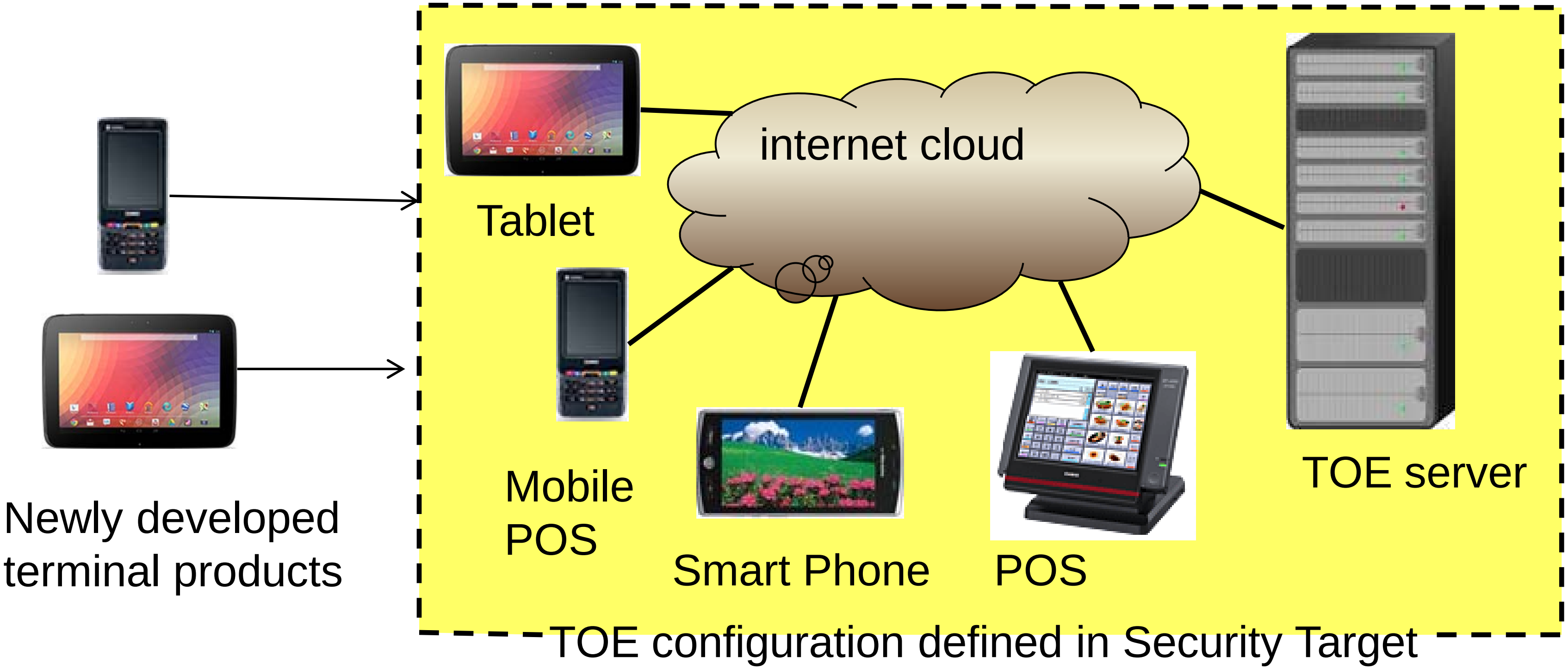
Applying Common Criteria to a cloud type payment service

Kenji Yamaya

ECSEC Laboratory Inc.

Evaluation of a cloud system


internet cloud
Tablet
Mobile POS
Smart Phone
POS
TOE server
Newly developed terminal products
TOE configuration defined in Security Target

- A cloud system we evaluated varies dynamically by terminals connected with.
- The configurable TOE is one reason to the difficulty in evaluating the cloud system.

Contents

Thincacloud and its evaluation

Idea for whole cloud evaluation

Evaluation of terminals

Evaluation of a server

Evaluation of a whole cloud system

Remaining issue

Conclusion

Contents

- **Thincacloud and its evaluation**
- **Idea of whole cloud evaluation**
  - **Evaluation of terminals**
  - **Evaluation of a server**
  - **Evaluation of a whole system**
- **Remaining issue**
- **Conclusion**

What is Thincacloud

- Thincacloud is a **cloud system based on NFC** solution.
- It is currently available and providing e-commerce payment service in Japan.
- No evaluation regarding whole cloud system evaluation including many kinds of terminals, so far.

What is Thincacloud

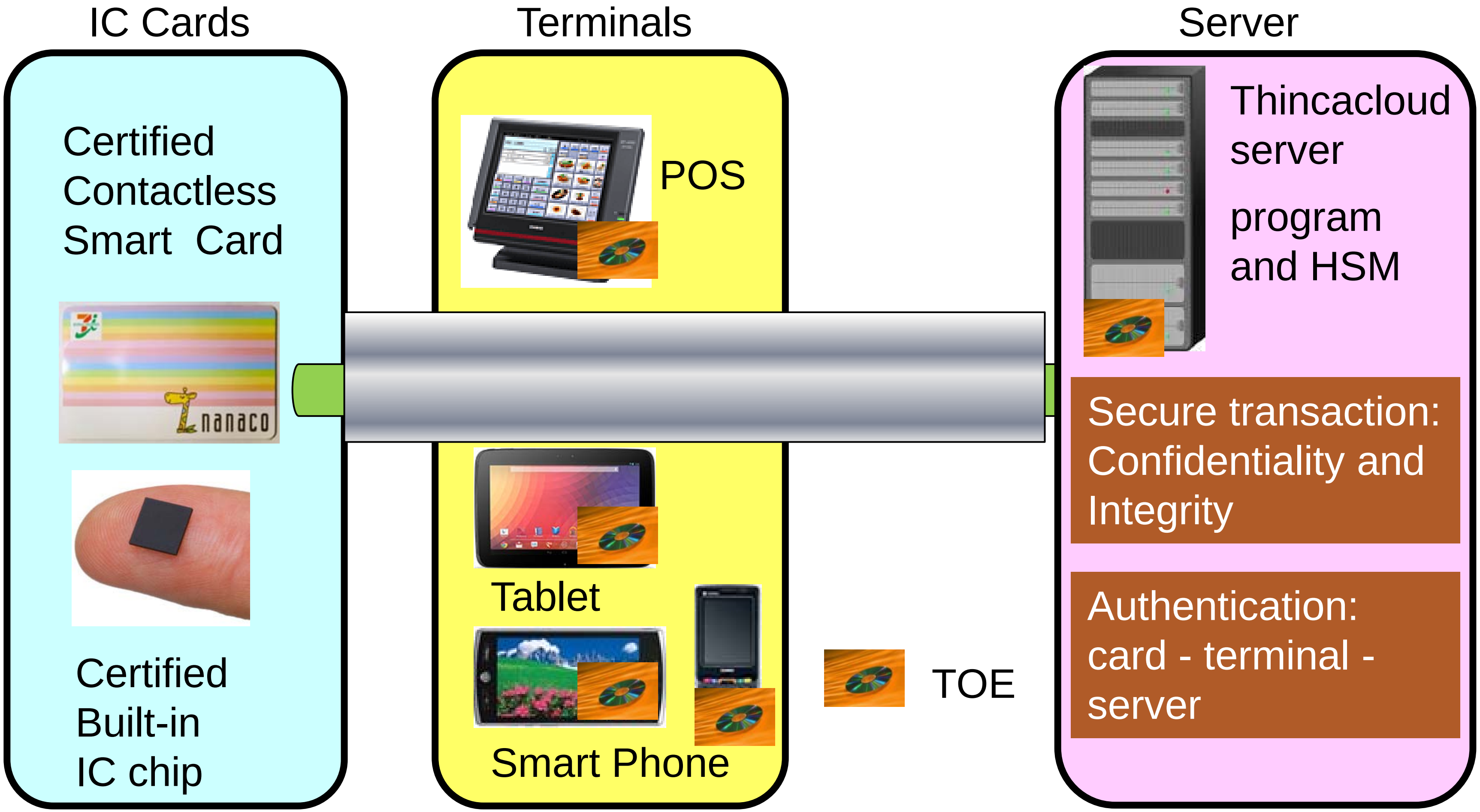
Real payment

Virtual payment

At restaurants
At shops
In a taxi
Delivery Services

By TV
By Smart Phones
In offices
By Tablets

Thincacloud architecture



IC Cards

Certified Contactless Smart Card

Certified Built-in IC chip

Terminals

POS

Tablet

Smart Phone

TOE

Server

Thincacloud server

program and HSM

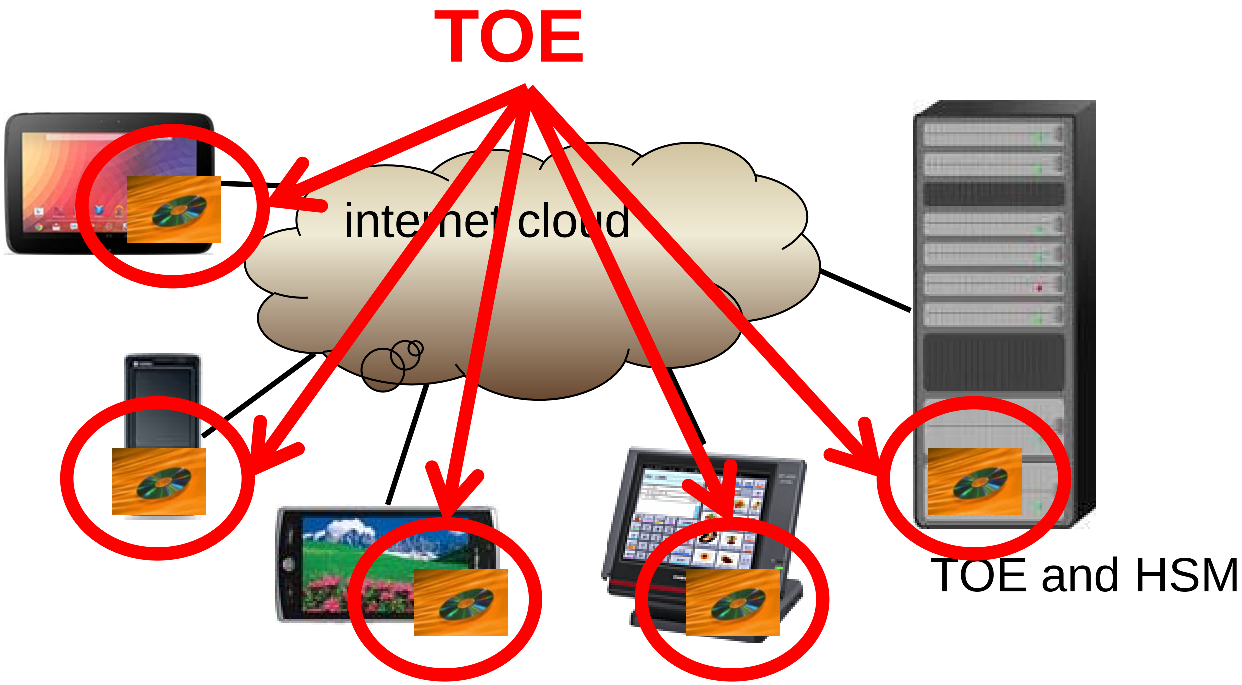
Secure transaction: Confidentiality and Integrity

Authentication: card - terminal - server

Merit of Thincacloud architecture

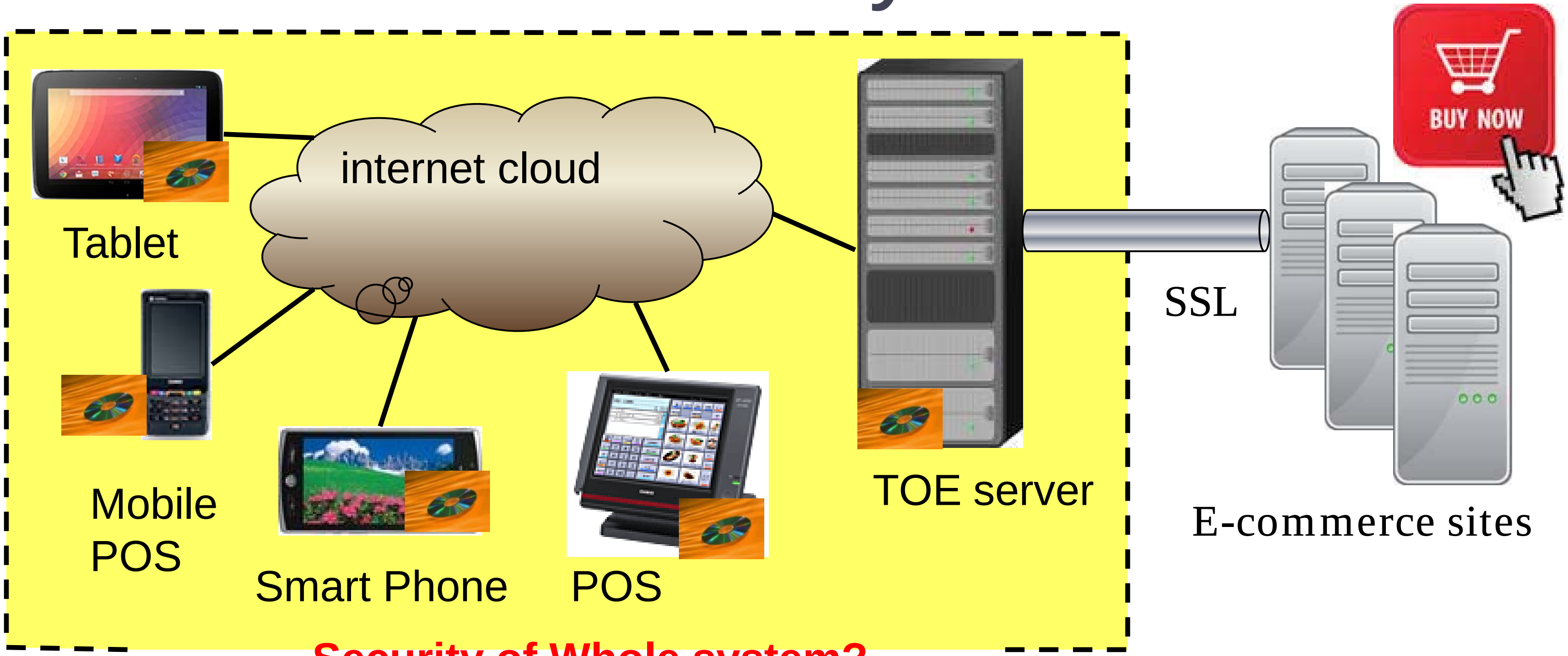
- Main security functionality is the secure session. The developer forces the secure session on the just High-EAL IC and the server.
- Terminals only support the secure session.
- The developer decides that TOE in terminals is a program, and configurable parts (OS and hardware) are IT environments.
- Therefore, assurance will be continued regardless of terminals until the program is updated.

Evaluated Thincacloud



- This TOE we have already evaluated is a small program in terminals and a program, and a HSM in a server.
- Merit : **Assurance will be continued regardless of terminals until the program is updated.**

How about a whole system ?



Security of Whole system?

- “Is my tablet secure to use Thincacloud payment?” some users may think.
- “Is my POS terminal secure?” some shop owners may think.
- “Is Thincacloud server secure?” e-commerce site owners may think.

Contents

- Thincacloud and its evaluation
- Idea for whole cloud evaluation
  - Evaluation of terminals
  - Evaluation of a server
  - Evaluation of a whole system
- Remaining issue
- Conclusion

Evaluation of terminals

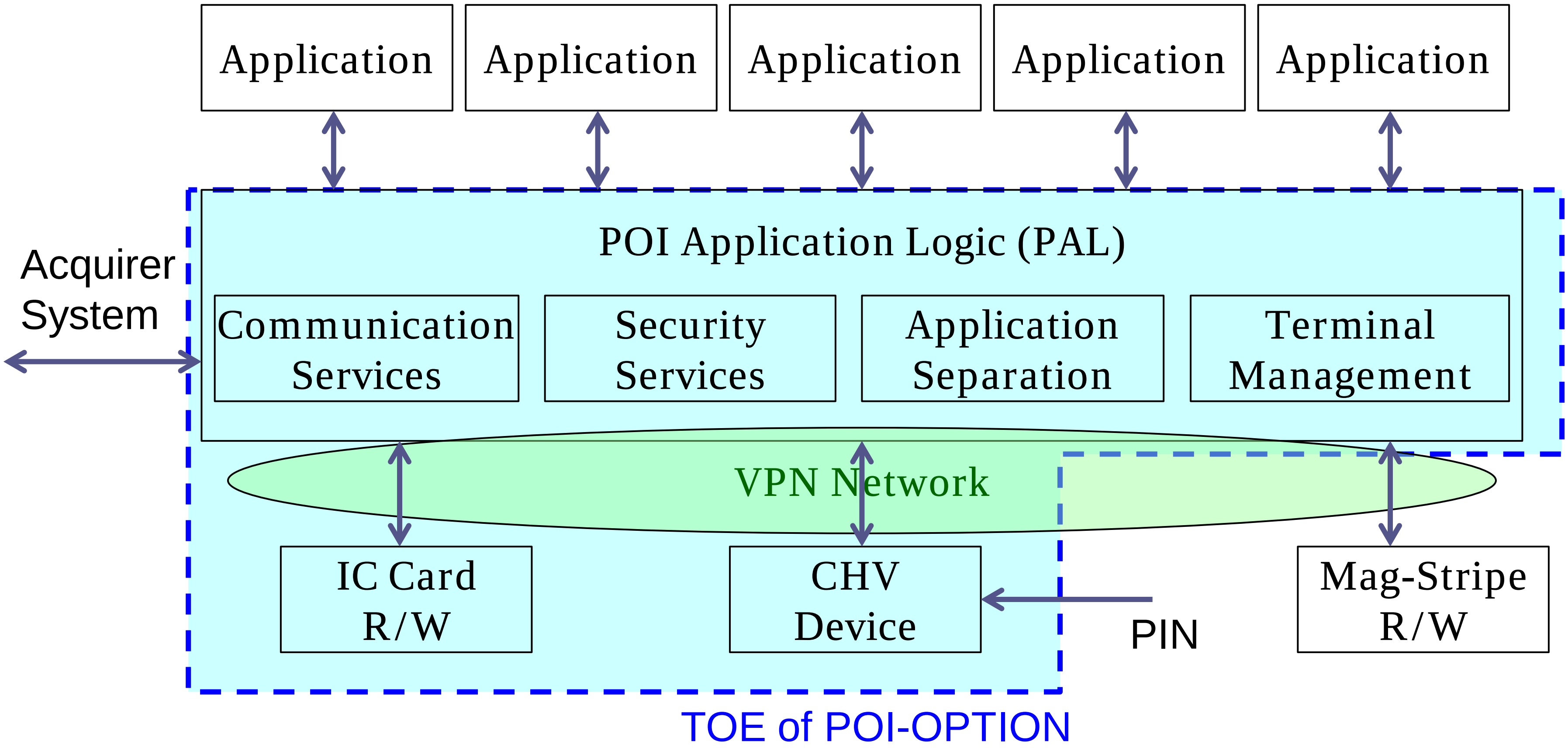
- How does the stakeholders obtain security assurance of the entire terminal, instead of a program?

- Is the Point of interaction protection profile (POI-PP) available for evaluation of the entire terminal?

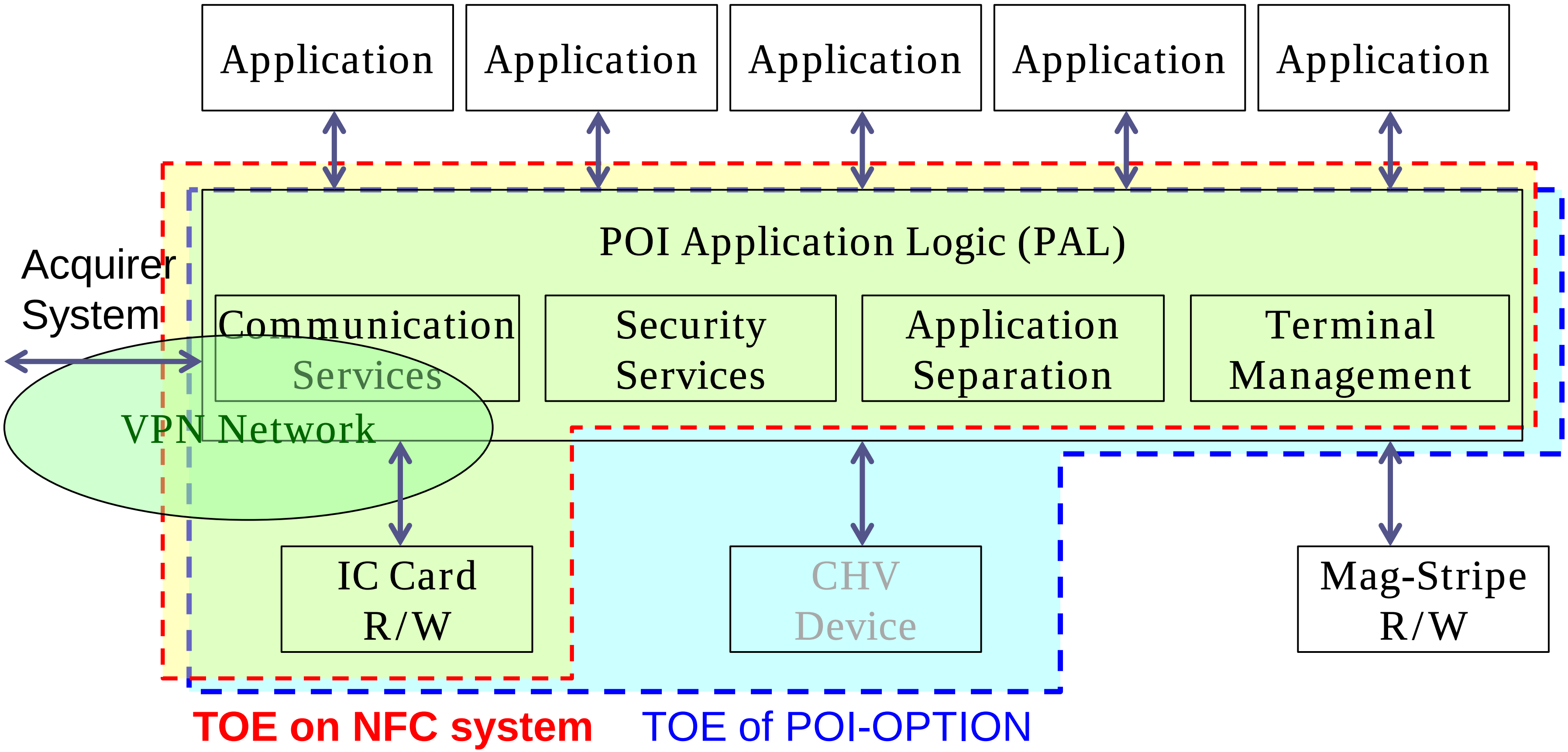
What is POI-PP

- **POI-PP** is a protection profile for the payment terminals, Version 2.0 certified by ANSSI on 2011.
- The target products are payment terminals with the smart card based transaction capability.
- POI-OPTION configuration: TOE provides protection for smart card based transaction, payment transaction data management and external communication facilities.

POI-OPTION configuration



NFC configuration

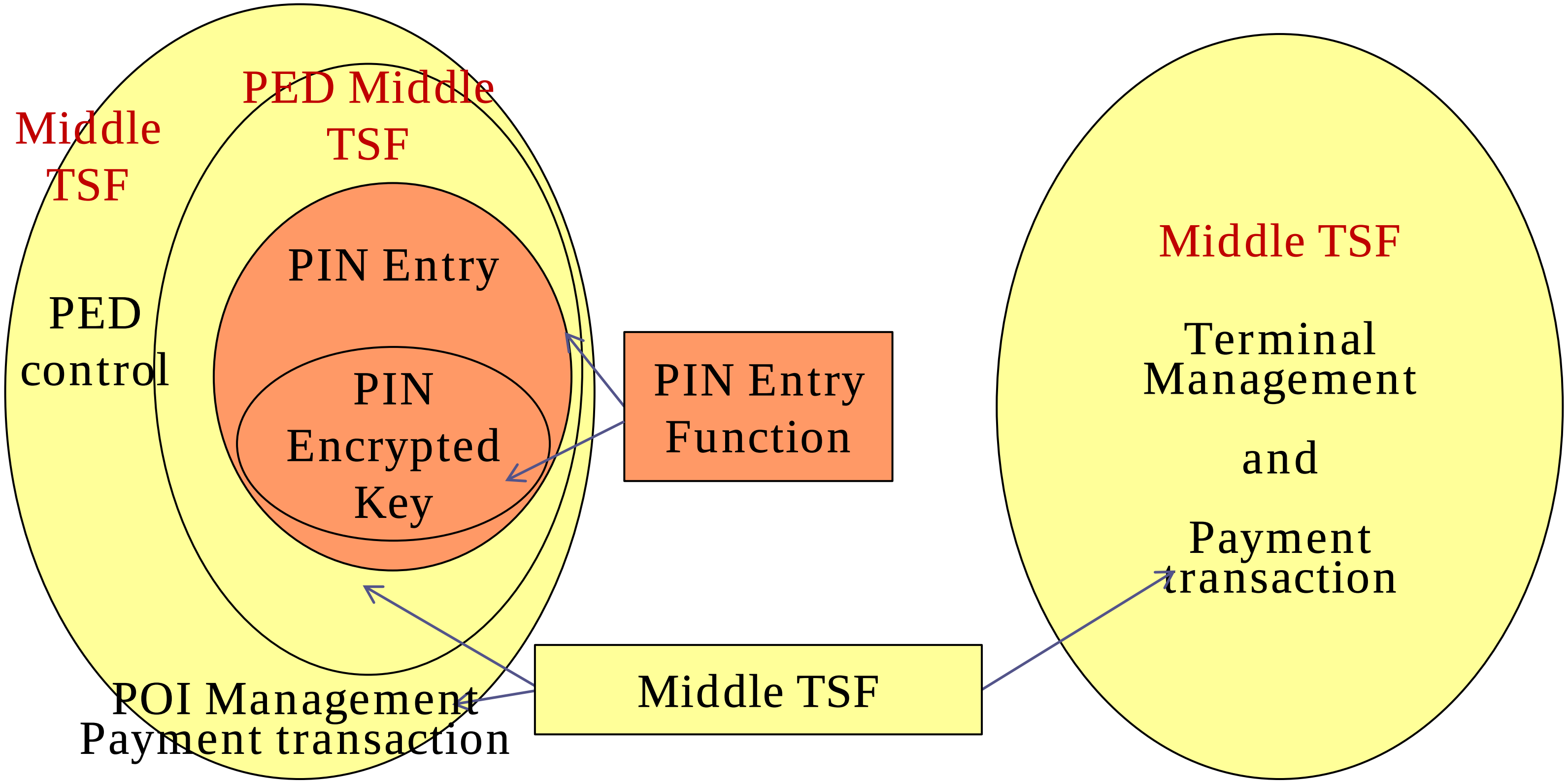


TOE on NFC system is similar to one of POI-OPTION, which indicates that POI-PP could be applied to cloud system based on NFC.

TSF structures

POI-OPTION

NFC terminal



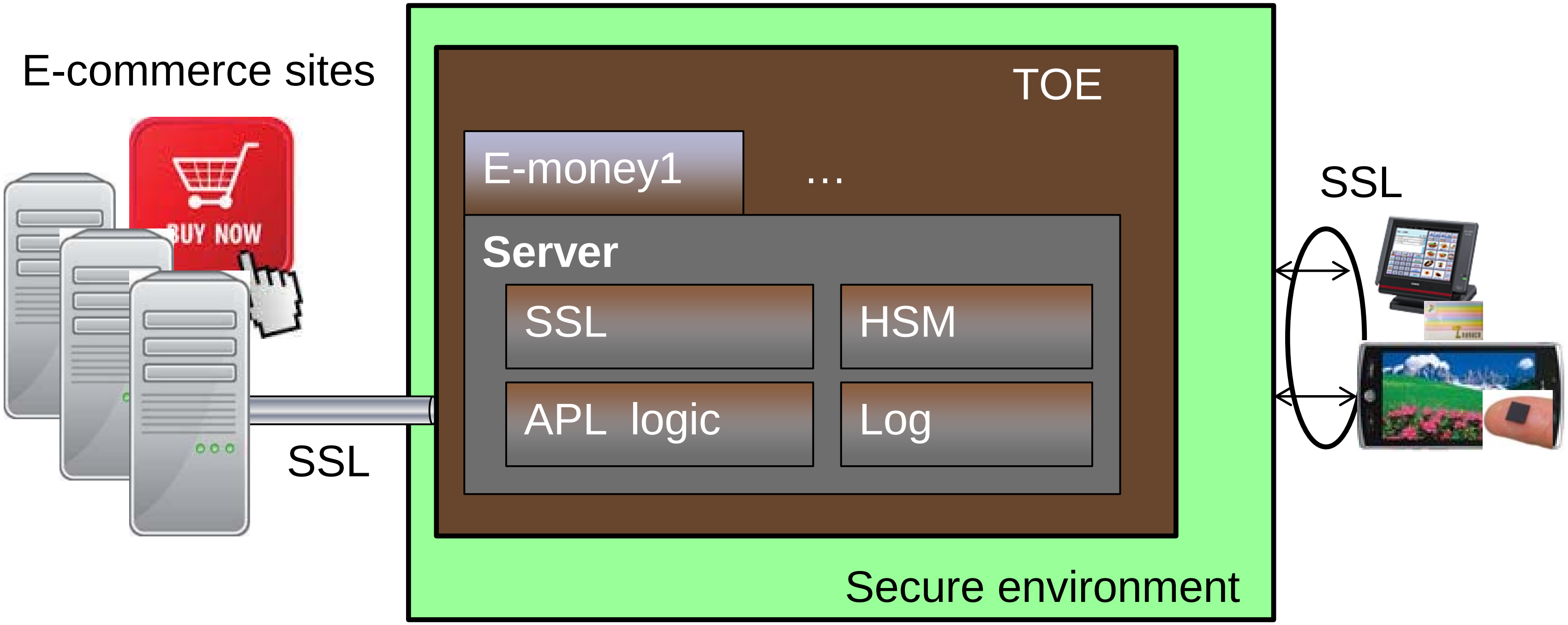
TSF based on NFC could be covered with POI-OPTION without PIN entry.

Contents

- Thincacloud and its evaluation
- Idea for whole cloud evaluation
  - Evaluation of terminals
  - Evaluation of a server
  - Evaluation of a whole system
- Remaining issue
- Conclusion

Evaluation of a server

- How the stakeholders obtain security assurance of total server instead of component only.



Evaluation of a server

- How the stakeholders obtain security assurance of **total server scheme** instead of component only.

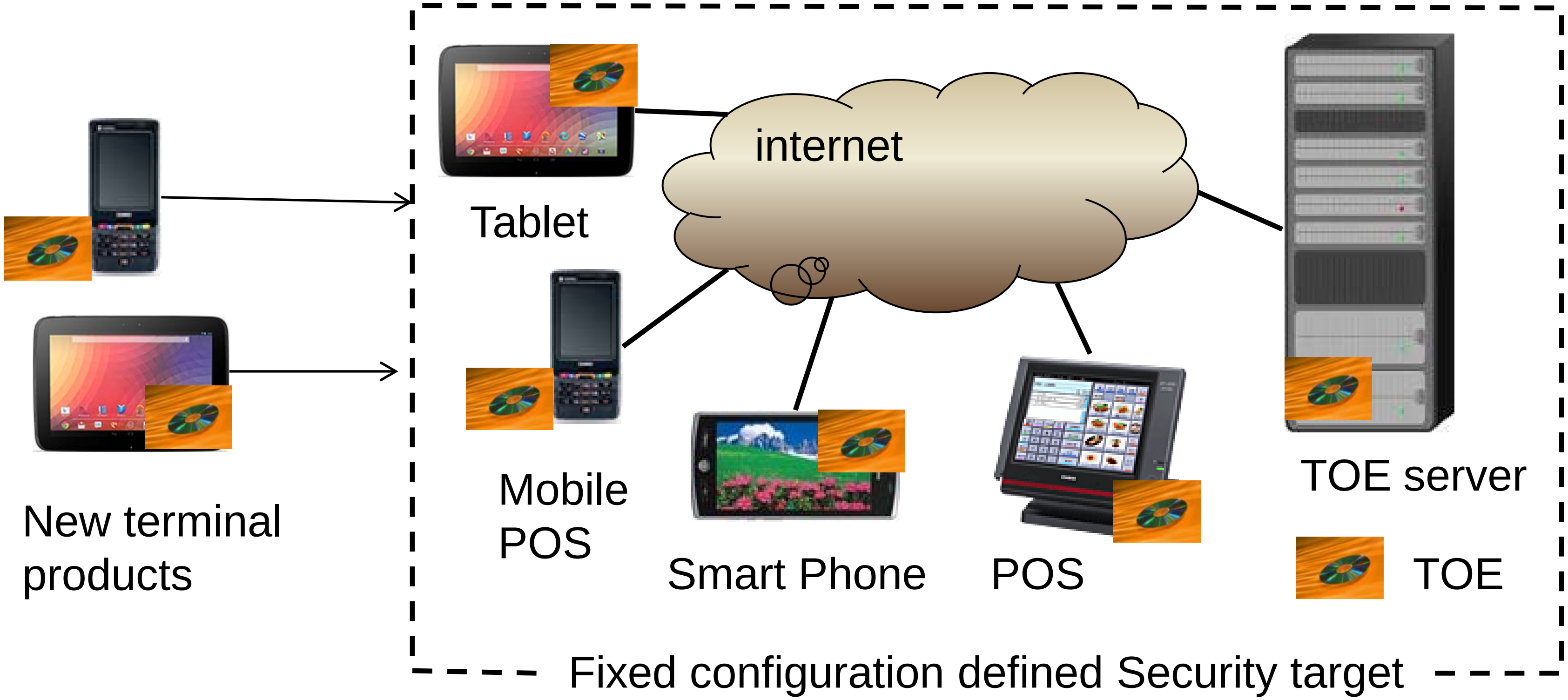
- Physical scope of the server-side TOE is total server including databases, HSMs, SSL accelerators, Web servers and so on.

Assurance continuity can be applied to the total server scheme, even when components are upgraded.

Contents

- Thincacloud and its evaluation
- **Idea for whole cloud evaluation**
  - Evaluation of terminals
  - Evaluation of a server
  - **Evaluation of a whole system**
- Remaining issue
- Conclusion

Evaluation of a whole system



- The client TOE runs well on the newly-developed terminals.
- **Rapid assurance continuity** is useful for whole system evaluation.

Evaluation of a whole system

- Security target describes the newly-developed terminal as a part of TOE.
- Evaluation of the newly-developed terminal is required.
  - From whole system point of view, evaluation of terminal means partial evaluation.

Then assurance continuity for the TOE is maintained and available for evaluation.

Contents

- Thincacloud and its evaluation
- Idea for whole cloud evaluation
  - Evaluation of terminals
  - Evaluation of server
  - Evaluation of whole system
- **Remaining issue**
- Conclusion

Remaining issue

- The e-commerce site is out of the scope of TOE.
- It is regarded as a user for the TOE.
- However, the card holder may require it is secure.

We need to consider how we assure the e-commerce site is secure enough.

Contents

- Thincacloud and its evaluation
- Idea for whole cloud evaluation
  - Evaluation of terminals
  - Evaluation of a server
  - Evaluation of a whole system
- Remaining issue
- **Conclusion**

Conclusion

- Idea of assurance for the whole cloud system including terminals.
  - ▫ Terminals: terminals are evaluated and applied for assurance continuity.

    Developing subset of **POI-PP TOE** might be applicable.
  - ▫ Server: **Total server scheme** as TOE is suitable for evaluation, NOT component base.
  - ▫ Whole system: **Rapid assurance continuity** could be useful depends on component's life cycle.

Thank you

ECSEC Laboratory Inc.

3-21, Kanda-Nishikicho, Chiyoda-ku
Tokyo, Japan 101-0054
TEL: +81-3-5259-8061 FAX: +81-3-5259-8070
E-mail: labinquiry@ecsec.jp

Evaluation of software / hardware IT Products by ISO/IEC15408
Testing of cryptographic module and algorithm implementation
by FIPS 140-2 and JIS X 19790 (ISO/IEC 19790)