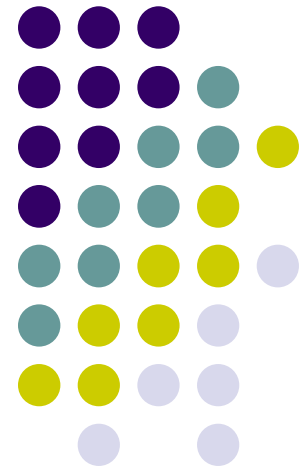




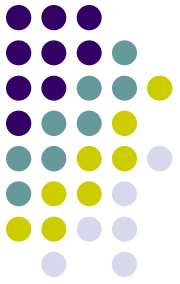
# Success of a smartcard composite TOE evaluation performed by NTTDATA

Naohisa ICHIHARA  
Research & Development  
Headquarters  
NTTADATA, JAPAN

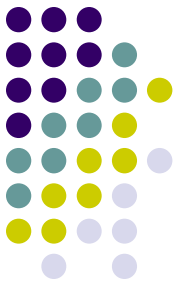




# Contents

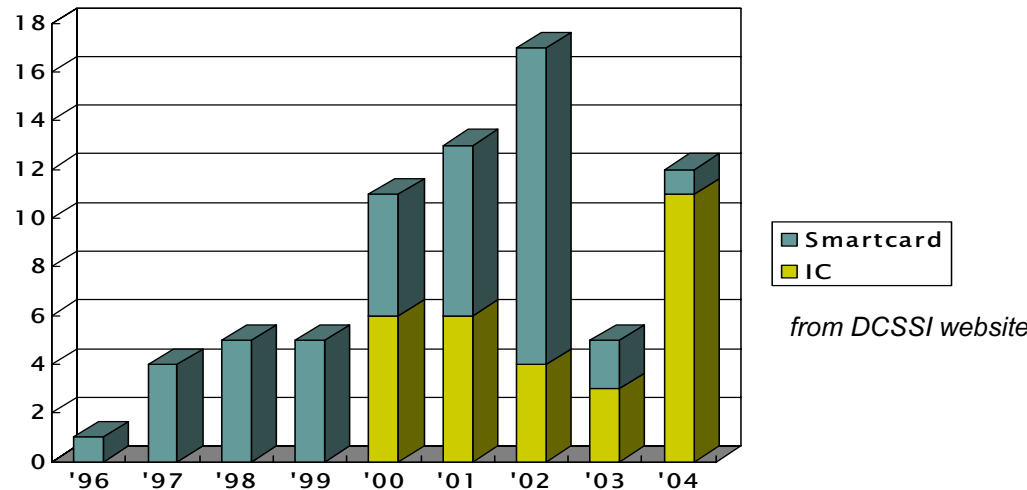


1. History of smartcard evaluation
2. Composite evaluation for smartcard
3. Typical case
4. Our case
5. Points
6. Conclusion



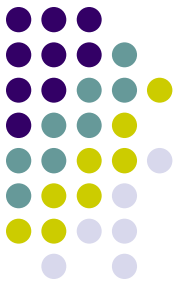
# History of smartcard evaluation

- 1996, The first successful case of smartcard evaluation
- 1998, CC v2.0 issued
- 1999, ISO/IEC adopted CC v2.0 as #15408
- 2000, The first successful case of IC evaluation
- 2002, **JIL document** issued, as CC supporting document  
*e.g. "ETR-lite for composition: Annex-A Composite smartcard evaluation: Recommended practice"*



from DCSSI website

Certified Products of IC, Smartcard



# Composite evaluation for Smartcard

- Why is CC evaluation needed for SC?
  - Customer's requirement
  - SC tends to be vulnerable as time goes by
  - Improve security skills of developers
  - High EAL contributes to low cost as well as high security
- Why is the Composite evaluation used for SC?
  - Saving time and cost of evaluation
  - Implemented with multiple components
  - Developed by multiple vendors
  - Used as one product in real service



# Composite evaluation for Smartcard



- What is 'composite evaluation' on earth?
  - Evaluation of underlying product e.g. IC
  - Evaluation of 'Composite product' e.g. Smartcard
    - Composite ST based on ST-lite (+ compatible PPs)
    - Composition Activities
    - Available to use ETR-lite

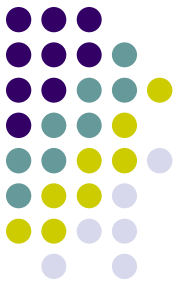


# Composite evaluation for Smartcard

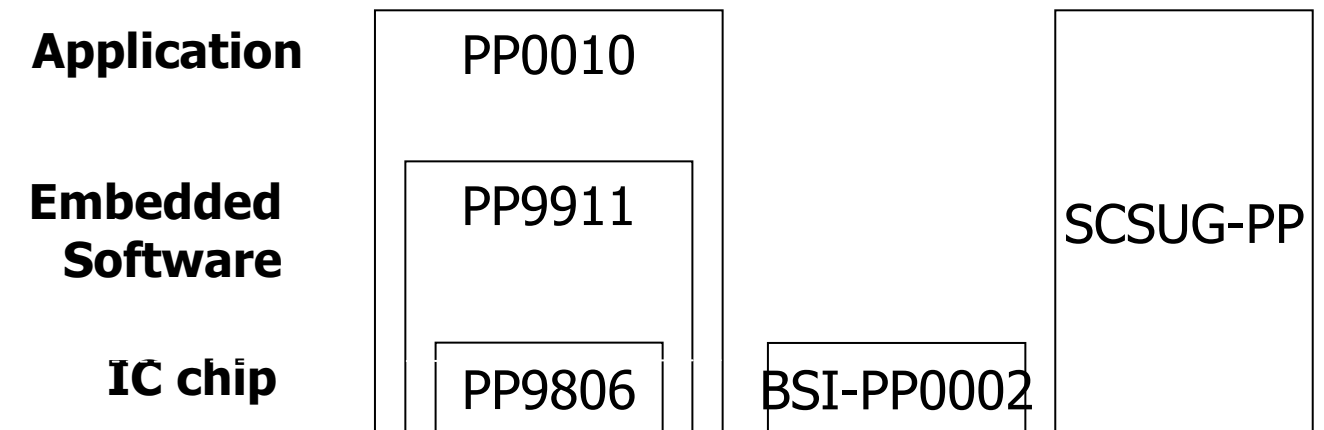
- *Composition activities ... " in order to verify that weaknesses are not introduced by the integration of the composite product"*
  - ASE: "evaluation of composite product ST", "use of ST-lite"
  - ACM: "Integration of Embedded Software in the IC manufacturer configuration management system"
  - ADO: "Consistency check for delivery and pre personalization procedures"
  - ADV: "Compliance with the IC developer recommendations"
  - ATE: "Composite product functional testing"
  - AVA: "Composite product vulnerability analysis"
  - Use of ETR-lite

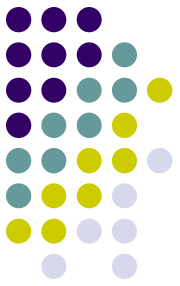


# Composite evaluation for Smartcard



- PP compliance
  - Composite PP (like PP9911/PP0010) is made by keeping compliance with underlying PP (like PP9806)



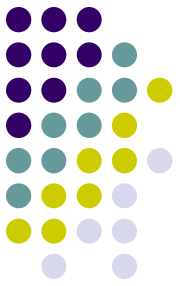


# Composite evaluation for Smartcard

- ST-lite
  - Such ST is needed only for
    - another evaluation (for the reference and reuse of evaluation result)
    - product user (disclosure)
- ETR-lite
  - Such ETR is needed only for
    - another evaluation (for the reference and reuse of evaluation result)



# Typical case 1

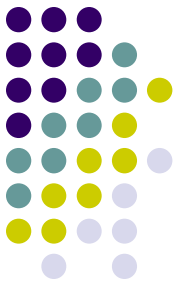


- Simplest case

	IC evaluation	Composite evaluation
CB	CB1 (in country C1)	CB1
PP referred in ST	PP1	PP2
Number of developer	1	1
Developer's country	C1	C1 or another
PP compliance	Yes	



## Typical case 2

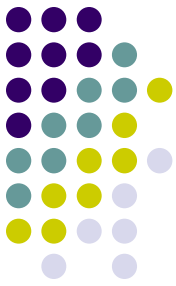


- Two different CBs are involved
- For CB2, ETR-lite could be available

	IC evaluation	Composite evaluation
CB	CB1 (in country C1)	CB2 (in country C2)
PP referred in ST	PP1	PP2
Number of developer	1	1
Developer's country	C1	C1 or another
PP compliance	Yes	



## Our case



- The first challenge of composite evaluation
- 'ST evaluation' is required by user before Aug. 2003
- Scope: TOE = IC + ES + 2APs (initially)

	IC evaluation	Composite evaluation
CB	France	France
PP refered in ST	PP9806	JUKI-PP
Number of developer	1	2
Developer's country	France	Japan
PP compliance	No	



# Points to succeed



- How to handle ST without PP compliance
- How to apply CC for complicated formation of development
- How to achieve ALC, ACM, ADO for Japanese developers' project as well as for development site visit by foreign ITSEF
- Coordination with all related protagonists

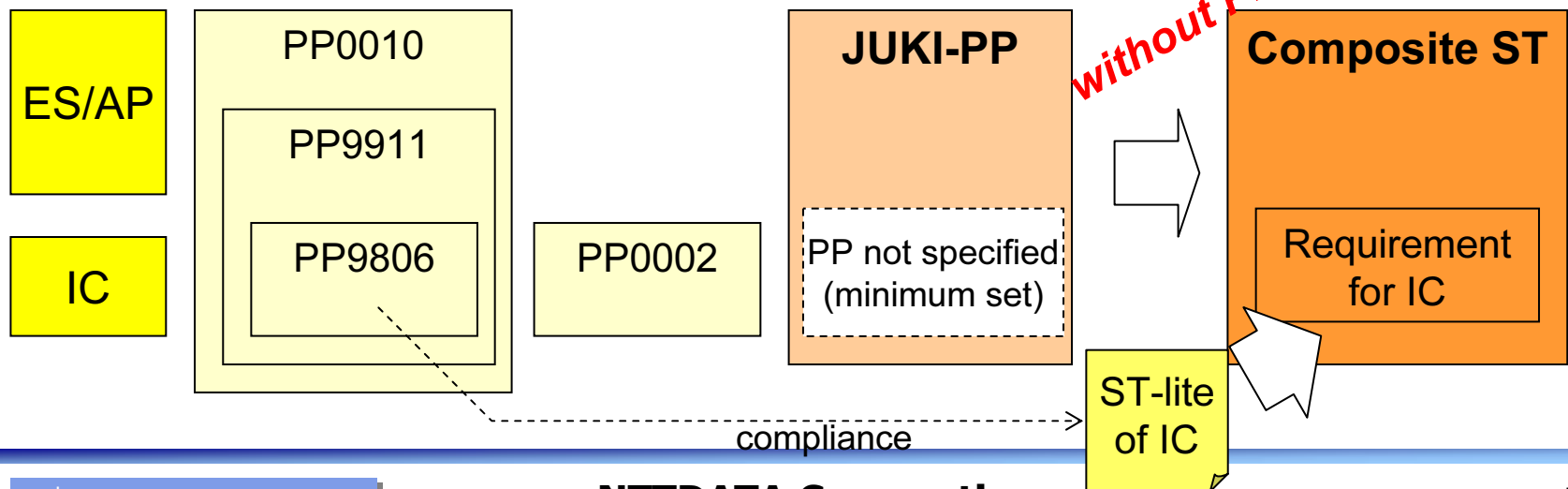


# Point #1 ST



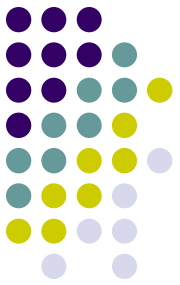
## ISSUE

- JUKI-PP defines only a minimum set of requirements (SFRs)
- ST is required to be compliant with JUKI-PP
- Contents of ST must be adapted



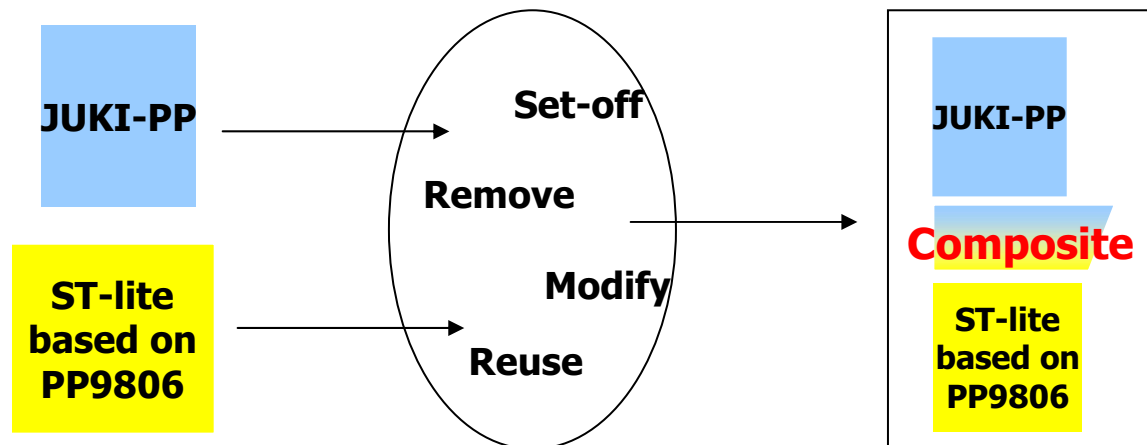


# Point #1 ST



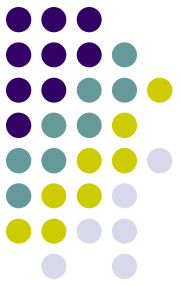
## SOLUTION

- ST adaptation
  - Method for reusing, removing, modifying or set-off of security environments and security functional requirements for both STs
    - *"A new methodology for composite smartcard evaluation", N.Ichihara, NTTDATA, ICC2003*





# Point #2 Three-layered TOE

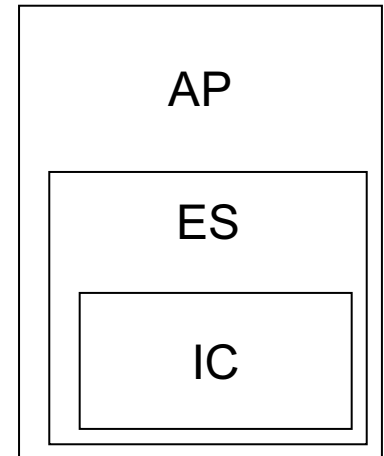


## ISSUE

- TOE includes IC + ES + AP
- Security Functional Requirement for ?
- Identification of security for each of them

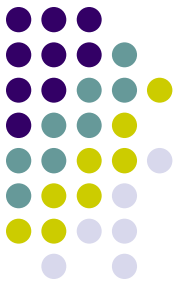
### ● *Composition Activities*

- *ASE: “Evaluation of composite product ST”, “use of ST-lite”*
- *ADV: “Compliance with the IC developer recommendations”*
- *ATE: “Composite product functional testing”*



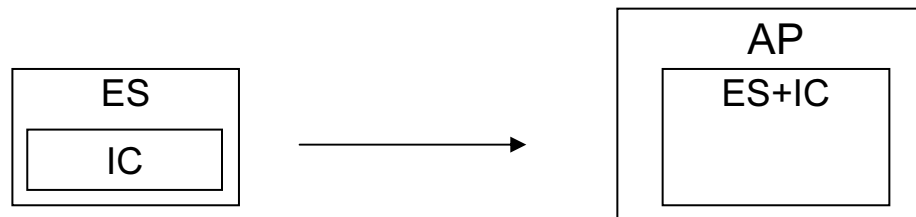


# Point #2 Three-layered TOE



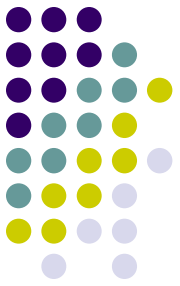
## SOLUTION

- “Internal composite evaluation”
  - Identifying the boundary of security responsibility for each one
  - Composite evaluation for “IC+ES”
    - ES compliance with security recommendations provided by IC
    - Security recommendations of ES to ES users / AP developer
  - Composite evaluation for “AP+ result of composite evaluation of IC+ES”
    - AP compliance with security recommendations provided by ES and IC
    - Security recommendations of AP to AP users



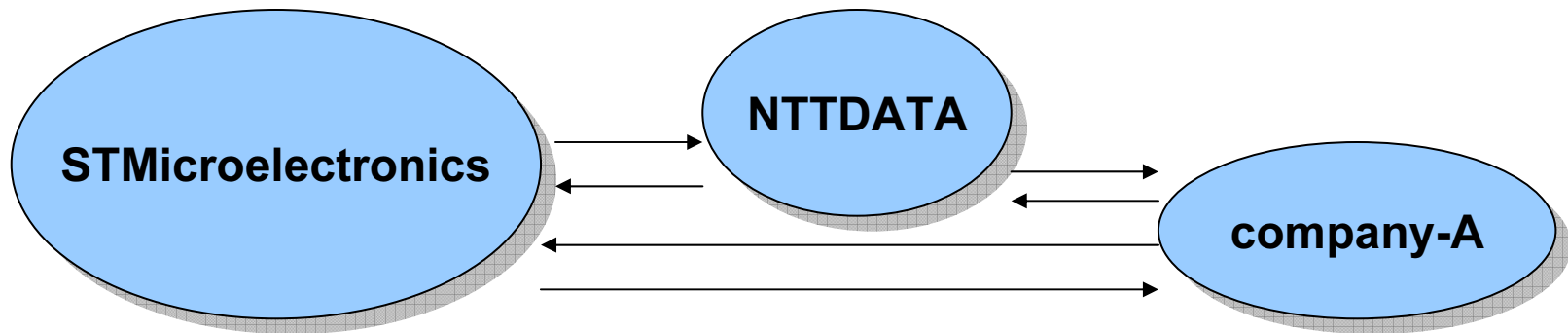


# Point #3 Complicated formation



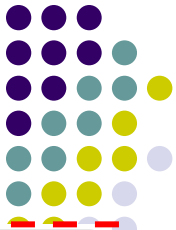
## ISSUE

- How to apply methodology of 'composite evaluation' to our case?
  - IC developer/manufacturer: STMicroelectronics
  - ES developer/designer: NTTDATA
  - ES coding/card manufacturing: company-A





# Point #3 Complicated formation



## SOLUTION

- To define roles and responsibilities
- To assign developers to related roles for each lifecycle stage
- To apply composition activities (ALC, ACM, ADO)
- Then, ITSEF could identify *'Who' should be checked on 'what' kind of activity?*

Phase 1	Smartcard embedded software development	<b>the smartcard embedded software developer</b> is in charge of the smartcard embedded software development and the specification of IC pre-personalisation requirements,
Phase 2	IC development	<b>the IC designer</b> designs the IC, develops IC dedicated software, provides information, software or tools to the smartcard embedded software developer, and receives the smartcard embedded software from the developer, through trusted delivery and verification procedures. From the IC design, IC dedicated software and smartcard embedded software, he constructs the smartcard IC database, necessary for the IC photomask fabrication,
Phase 3	IC manufacturing and testing	<b>the IC manufacturer</b> is responsible for producing the IC through three main steps : IC manufacturing, IC testing, and IC pre-personalisation,
Phase 4	IC packaging and testing	<b>the IC packaging manufacturer</b> is responsible for the IC packaging and testing,
Phase 5	Smartcard product finishing process	<b>the smartcard product manufacturer</b> is responsible for the smartcard product finishing process and testing,
Phase 6	Smartcard personalisation	<b>the personaliser</b> is responsible for the smartcard personalisation and final tests. Other smartcard embedded software may be loaded onto the chip at the personalisation process,
Phase 7	Smartcard end-usage	<b>the smartcard issuer</b> is responsible for the smartcard product delivery to <b>the smartcard end-user</b> , and the end of life process.



# Point #3 Complicated formation

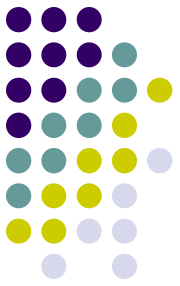


## SOLUTION

- Phase1
  - Role
    - ES developer = ES designer + ES implementer
    - ES designer: ES design and testing
    - ES implementer: ES coding and debugging
  - Corresponding composition activities
    - Development life cycle among 2 ES developers (ALC\_LCD)
    - Configuration management among 2 ES developers (ACM)
    - ES Delivery to IC manufacturer (ALC\_DVS, ADO\_DEL)



# Point #3 Complicated formation

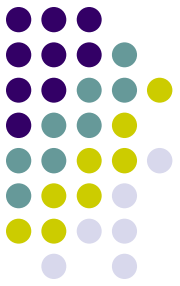


## SOLUTION

- Phase5
  - Role
    - Card manufacturer: Manufacturing and testing of smartcard
    - ES designer: Design of pre personalization data
    - Card initial issuer: Initial issue of smartcard
  - Corresponding composition activities
    - Reception of IC from IC developer (ADO\_DEL, ADO\_IGS)
    - Reception of pre personalization data (ADO\_DEL, ADO\_IGS)



# Point #4 ALC, ACM, ADO



## ISSUE

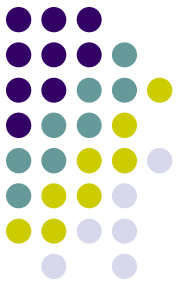
- Site audit by French ITSEF (**SERMA Technologies**)

**ALC\_DVS.2.2E** The evaluator shall confirm that the security measures are being applied.

- How can they *confirm*?
- It was not realistic to translate all pieces of evidences
  - Manual for Company's TQM / PM / Security policy
  - Ledger of project information, document, source code or product
  - Japanese tools for software development or configuration management
  - Explanations of security measures (safe-box, security door, ...)



# Point #4 ALC, ACM, ADO

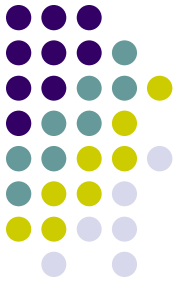


## SOLUTION

- (1) Outsourcing using Japanese ITSEF
  - **SERMA** subcontracts to the Japanese ITSEF (**ECSEC**) in order to perform partial documentary evaluation
  - ECSEC is recognized by the French CB **DCSSI**
  - We provide ECSEC with Japanese documents as it is
  - We make and provide English summary documents to SERMA
  - ECSEC checks Japanese documents and make report to be sent to SERMA, according to the result of check
  - SERMA checks reports from ECSEC as well as the consistency with the summaries

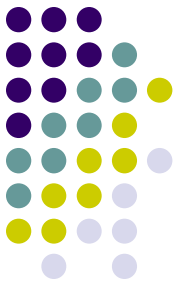


# Point #4 ALC, ACM, ADO



## SOLUTION

- (2) Site audit with ECSEC
  - Preliminary ITSEF meeting
  - Site audit with ECSEC as trusted translator
  - ITSEF Meeting after audit
  - Plenary meeting with developers and ITSEFs



## Point #5 Coordination

- Internally
  - on CC study, arrangement of site audit,
- with CB(DCSSI), ITSEF(SERMA)
  - on every 'points' before evaluation starts
- with Japanese ITSEF(ECSEC)
  - on outsourcing and contract
- with IC developer (STMicroelectronics)
  - on *specialized* 'composition activities' and roles
- with company-A
  - on CC study, preparation of deliverables, site audit,
- Miscellaneous
  - Presentation of new methodology (ICCC), to be discussed
  - Participating in WG (ISCI-WG1) , to share issues



# Conclusion

## Summary

- History and the origin of composite evaluation
- Important points:
  - ST, Complicated formation, ALC/ACM/ADO
  - Coordination with all involved parties

## Future works of NTTDATA

- CCv3.0 impact
- Harmonization with US, EU and Asian countries
- New methodology for security engineering
  - high security / low cost
  - early-built-in security
  - integrating with requirement/software engineering





# Question?

**Naohisa ICHIHARA**

e-mail : [ichiharan@nttdata.co.jp](mailto:ichiharan@nttdata.co.jp)

Research and Development Headquarters, **NTTDATA**

Special thanks to:

**Michael DULUCQ**, SERMA technology