March 2001

Tokyo Smartcard Security Conference

Smartcard Platform Certification Using the Common Criteria Issues & Opportunities

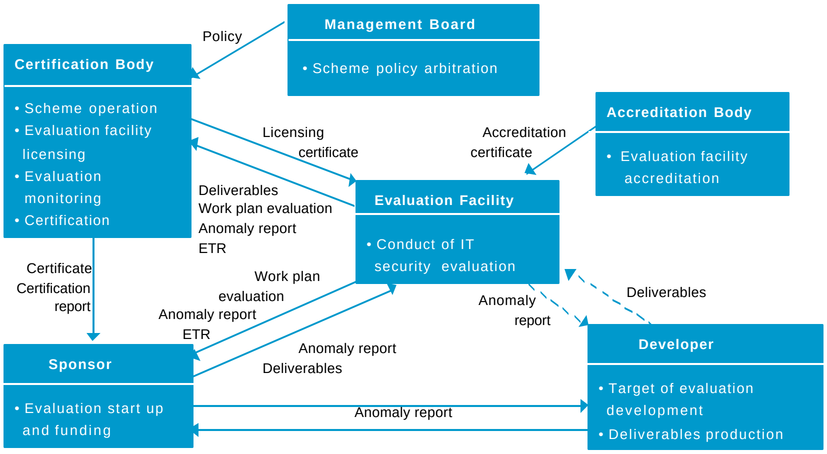
Alain Jarre

STMicroelectronics

Agenda

- ❑ Introduction
- ❑ Evaluation and Certification Parties
- ❑ From Protection Profile (PP) to Security Target (ST)
  - ✓ PP, TOE, Assurance level, Augmentation, ST
- ❑ Evaluation and certification process
- ❑ Examples & comments on CC & PP’s.
- ❑ New initiatives GlobalPlatform - eEurope
- ❑ Conclusions

Evaluation and Certification
The Scheme



Management Board
- Scheme policy arbitration

Policy

Certification Body
- Scheme operation
- Evaluation facility licensing
- Evaluation monitoring
- Certification

Accreditation Body
- Evaluation facility accreditation

Licensing certificate

Accreditation certificate

Deliverables
Work plan evaluation
Anomaly report
ETR

Evaluation Facility
- Conduct of IT security evaluation

Certificate
Certification report

Work plan evaluation
Anomaly report
ETR

Anomaly report
Deliverables

Anomaly report

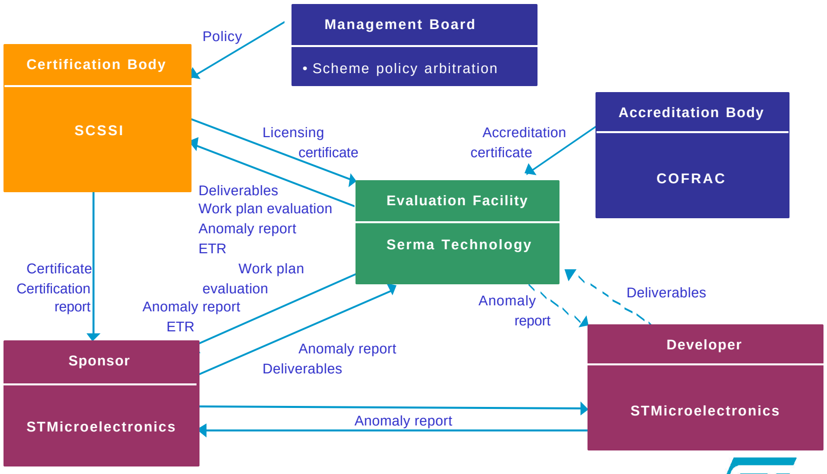
Deliverables

Sponsor
- Evaluation start up and funding

Developer
- Target of evaluation development
- Deliverables production

Anomaly report

Evaluation and Certification
example of partnership



Management Board
- Scheme policy arbitration

Policy

Certification Body
SCSSI

Accreditation Body
COFRAC

Licensing certificate

Accreditation certificate

Deliverables
Work plan evaluation
Anomaly report
ETR

Evaluation Facility
Serma Technology

Certificate
Certification report

Work plan evaluation
Anomaly report
ETR

Anomaly report
Deliverables

Anomaly report

Deliverables

Sponsor
STMicroelectronics

Developer
STMicroelectronics

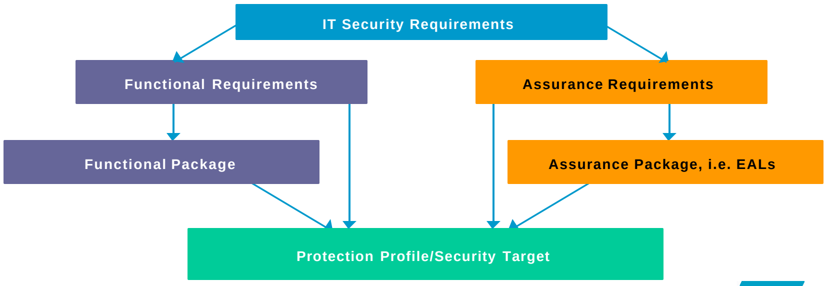
Anomaly report

Protection Profile

- ❑ What is a Protection Profile?
  - ✓ An implementation-independent set of Security Requirements for a category of products (TOEs) which meet specific *category of users* needs
- ❑ PP/9806 is the Protection Profile used up to now for Smartcard Ics.
- ❑ PP9911 is the one used for single applications
- ❑ Many others are under evaluation.
- ❑ Some PP's are used to "filter" the architectures and functional specifications. Open Kernel – MASSC (MedeaA1112)

Security Requirements

- ❑ Functional requirements
  - ✓ Desired security behavior of the TOE
- ❑ Assurance requirements
  - ✓ Grounds for confidence that the TOE meets its security objectives



Examples of Security Requirements

- ❑ Functional requirements
  - ✓ FIA – user identification and authentication before allowing use of other TOE security functions
  - ✓ FPT – notification of physical attack
    providing unambiguous detection of physical tampering

- ❑ Assurance requirements
  - ✓ ADV – stepwise refinement from the summary specification in the security target down to the actual implementation
  - ✓ AGD – understandability and coverage of the operational documentation provided by the developer

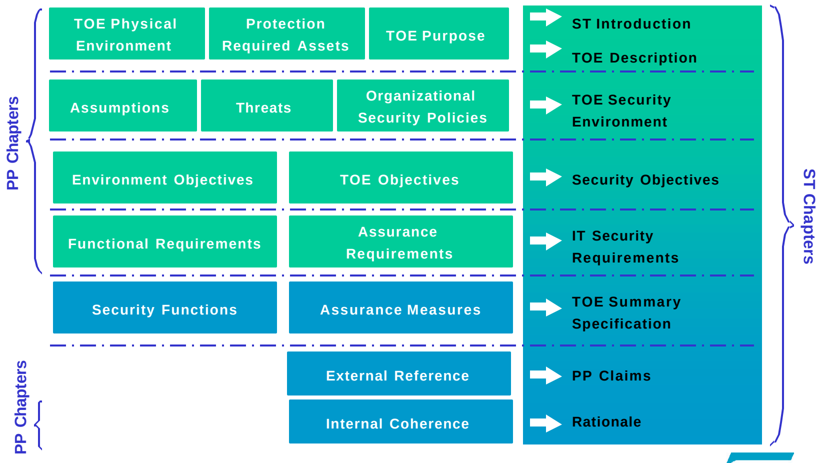
Assurance Level

- ❑ EAL7 = Formally verified design and tested
- ❑ EAL6 = Semi-formally verified design and tested
- ❑ EAL5 = Semi-formally verified design and tested
- ❑ **EAL4** = Methodically designed, tested and reviewed
- ❑ EAL3 = Methodically tested and checked
- ❑ EAL2 = Structurally tested
- ❑ EAL1 = Functionally tested

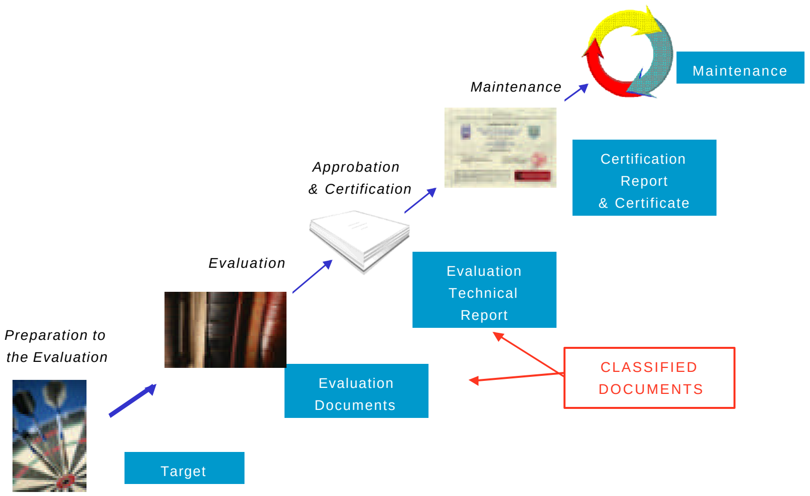
Augmentation

- Assurance requirements
  - ✓ Classes
    - ACM – Configuration management
    - ADO – Deliver and Operation
    - ADV – Development
    - AGD – Guidance documents
    - ALC – Life Cycle support
    - ATE – Tests
    - AVA – Vulnerabilities Assessment
  - ✓ Additional Assurance requirements for ST19SFxx platform (EAL4) are
    - ADV_IMP.2 (from EAL5)
    - ALC_DVS.2 (from EAL6)
    - AVA_VLA.4 (from EAL6)

From Protection Profile to Security Target



Evaluation / Certification Steps



Preparation to the Evaluation

Target

Evaluation

Evaluation Documents

Approbation & Certification

Evaluation Technical Report

Maintenance

Certification Report & Certificate

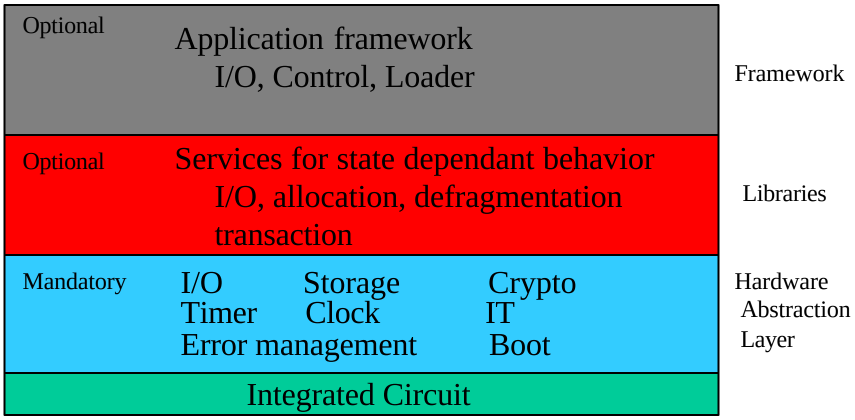
Maintenance

CLASSIFIED DOCUMENTS

Global Platform Card Committee

- ❑ OPEN KERNEL Working Group
- ❑ More representative of industry
- ❑ Chip manufacturers
  - ✓ Hitachi
  - ✓ Infineon
  - ✓ Philips
  - ✓ ST
- ❑ Card suppliers & Others
  - ✓ Bull
  - ✓ Datacard Platform 7
  - ✓ OCS
  - ✓ Gemplus

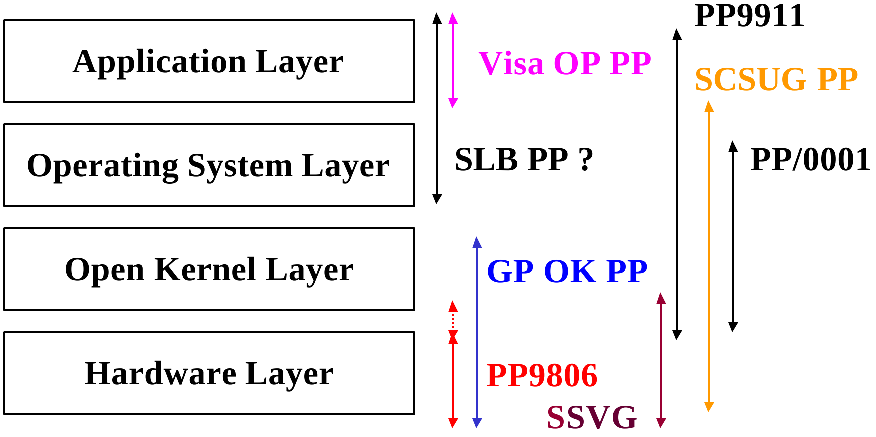
Open Kernel Architecture



List of OK deliverables

- ❑ OK general specification
  - ➪ *Blue layer specification: HAL*
  - ➪ Red layer specification: libraries
  - ➪ Black layer specification: framework
- ❑ OK Protection Profile
  - ➪ Guideline and/or Protection Profile
- ❑ *OK detailed specification: semi-formal model*
- ❑ *OK testing method*
  - ➪ *link with other working groups*

Overview the current PP’s scenario



Plus: MEDEA A112 PP’s and other applications PP’s

OK on security approach (1)

- ❑ Is a new PP really required ???
- ❑ PP: Security Functional +AssuranceRequirements
- ❑ No market standard requirements for security level.
- ❑ If PP: assumptions are necessary on upper levels
- ❑ A guideline defining security functions needed in OK will help to define new PP and even the ST.
- ❑ Both will perhaps be necessary

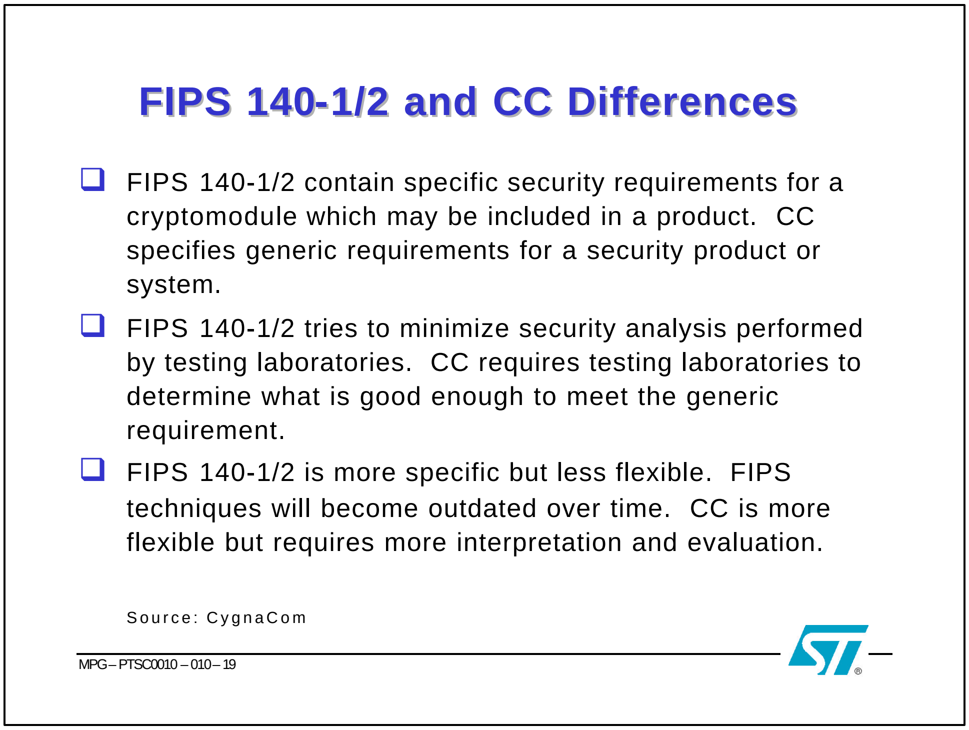
OK on security approach (2)

- ❑ Security issues are handled by security and Common Criteria expert members (some ESWGs).
- ❑ Plenary and dedicated meeting on the subject.
- ❑ Technical writing by Datacard experts (formal SW evaluators).

Another experience for cryptographic modules

- ❑ Summary of CygnaCom Experience in Developing Cryptography based Systems PPs and STs
- ❑ Examples of comparison with FIPS 140 .

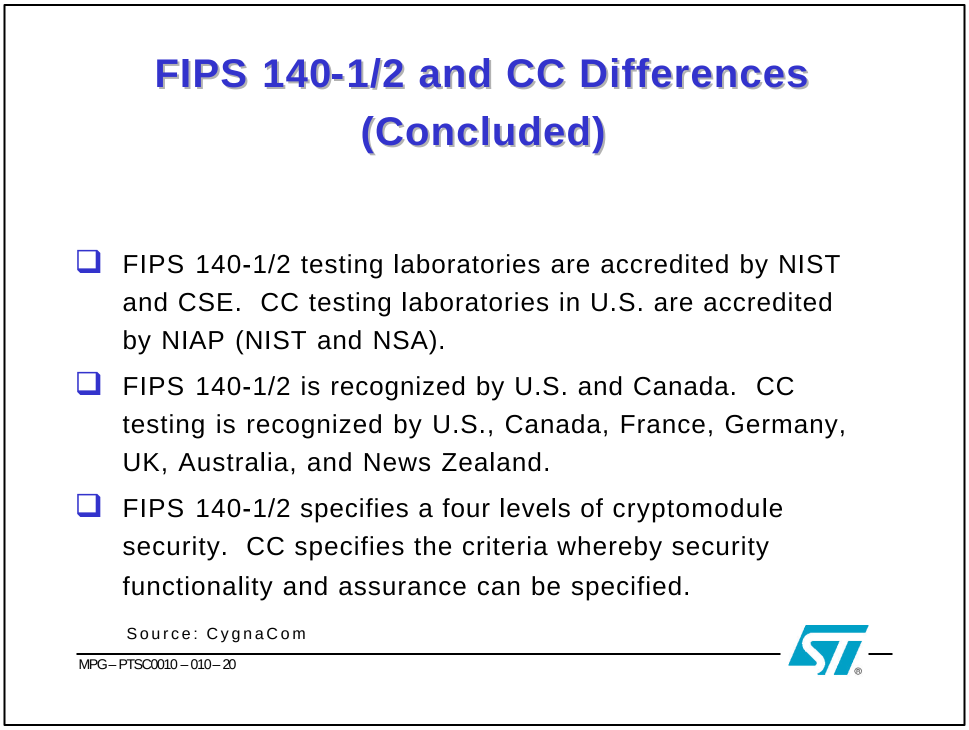
Source: CygnaCom



FIPS 140-1/2 and CC Differences

- FIPS 140-1/2 contain specific security requirements for a cryptomodule which may be included in a product. CC specifies generic requirements for a security product or system.
- FIPS 140-1/2 tries to minimize security analysis performed by testing laboratories. CC requires testing laboratories to determine what is good enough to meet the generic requirement.
- FIPS 140-1/2 is more specific but less flexible. FIPS techniques will become outdated over time. CC is more flexible but requires more interpretation and evaluation.

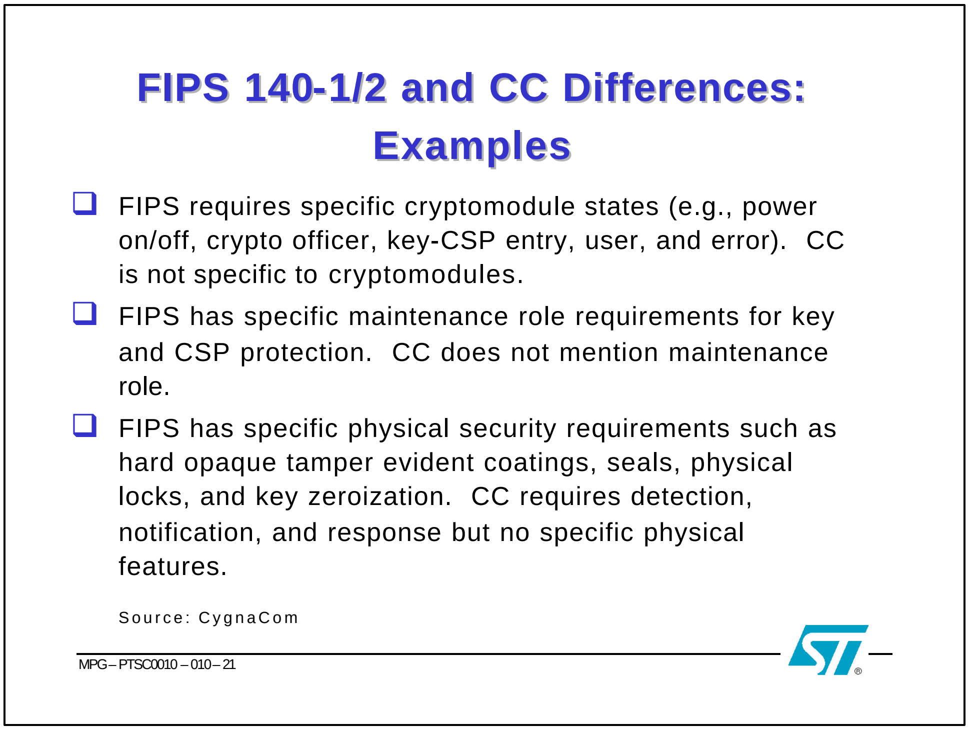
Source: CygnaCom



FIPS 140-1/2 and CC Differences (Concluded)

- FIPS 140-1/2 testing laboratories are accredited by NIST and CSE. CC testing laboratories in U.S. are accredited by NIAP (NIST and NSA).
- FIPS 140-1/2 is recognized by U.S. and Canada. CC testing is recognized by U.S., Canada, France, Germany, UK, Australia, and News Zealand.
- FIPS 140-1/2 specifies a four levels of cryptomodule security. CC specifies the criteria whereby security functionality and assurance can be specified.

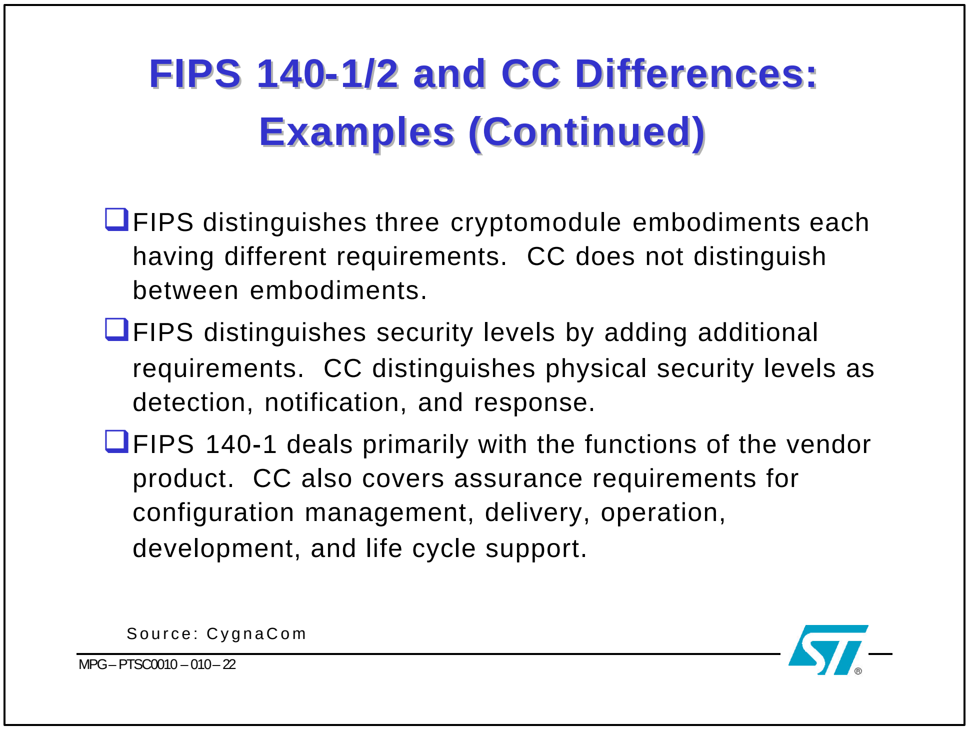
Source: CygnaCom



FIPS 140-1/2 and CC Differences: Examples

- ❑ FIPS requires specific cryptomodule states (e.g., power on/off, crypto officer, key-CSP entry, user, and error). CC is not specific to cryptomodules.
- ❑ FIPS has specific maintenance role requirements for key and CSP protection. CC does not mention maintenance role.
- ❑ FIPS has specific physical security requirements such as hard opaque tamper evident coatings, seals, physical locks, and key zeroization. CC requires detection, notification, and response but no specific physical features.

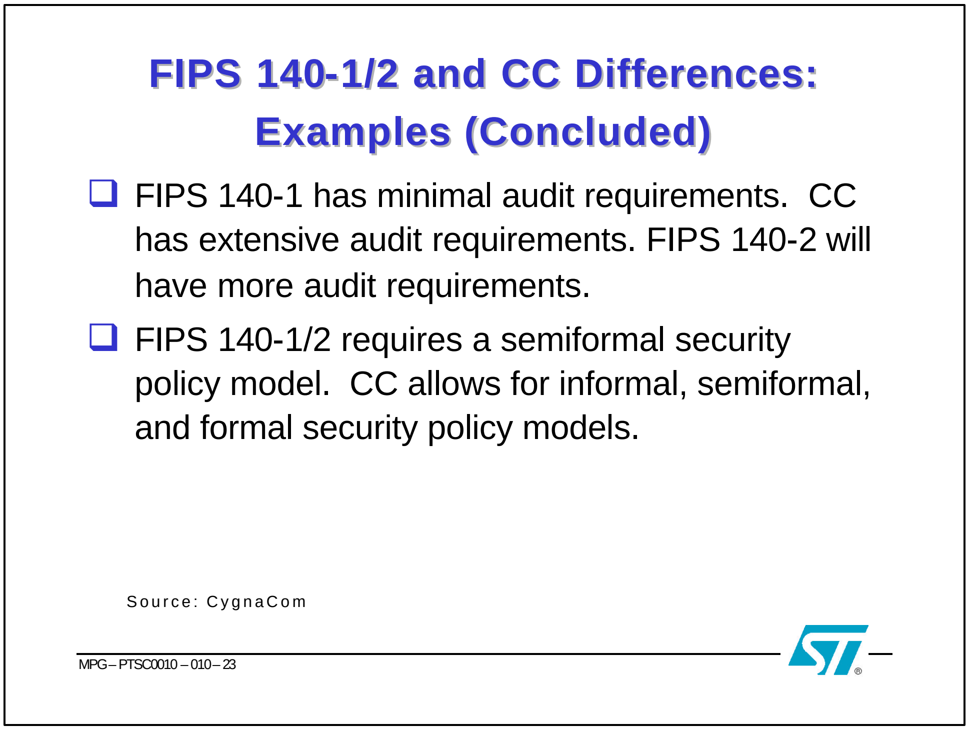
Source: CygnaCom



FIPS 140-1/2 and CC Differences: Examples (Continued)

- ❑ FIPS distinguishes three cryptomodule embodiments each having different requirements. CC does not distinguish between embodiments.
- ❑ FIPS distinguishes security levels by adding additional requirements. CC distinguishes physical security levels as detection, notification, and response.
- ❑ FIPS 140-1 deals primarily with the functions of the vendor product. CC also covers assurance requirements for configuration management, delivery, operation, development, and life cycle support.

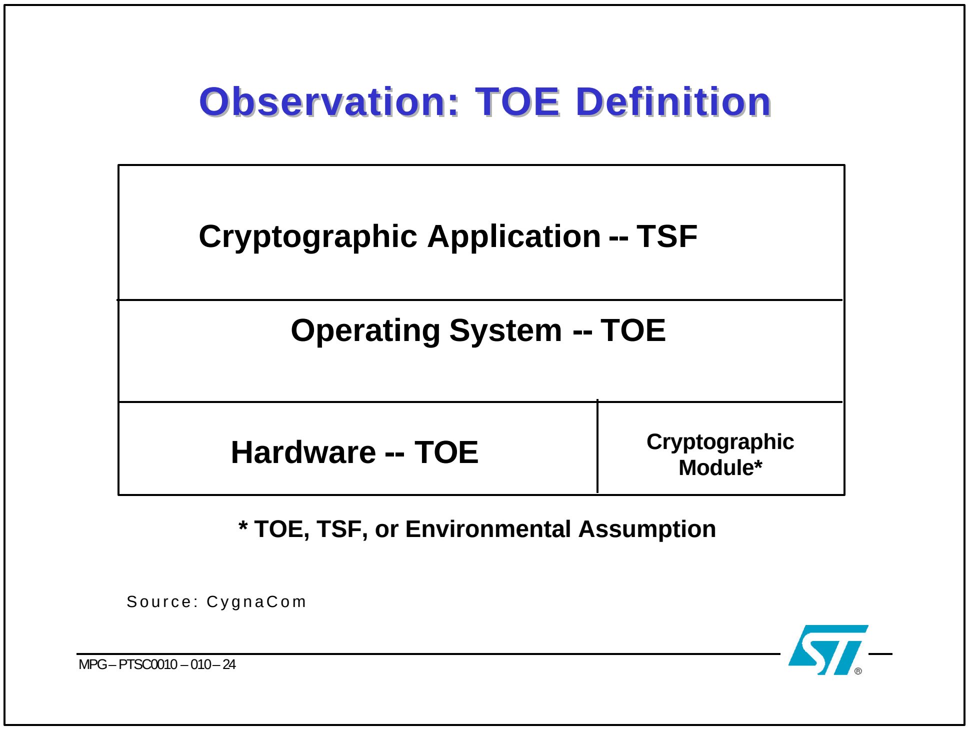
Source: CygnaCom



FIPS 140-1/2 and CC Differences: Examples (Concluded)

- ❑ FIPS 140-1 has minimal audit requirements. CC has extensive audit requirements. FIPS 140-2 will have more audit requirements.
- ❑ FIPS 140-1/2 requires a semiformal security policy model. CC allows for informal, semiformal, and formal security policy models.

Source: CygnaCom



Observation: TOE Definition

Cryptographic Application -- TSF

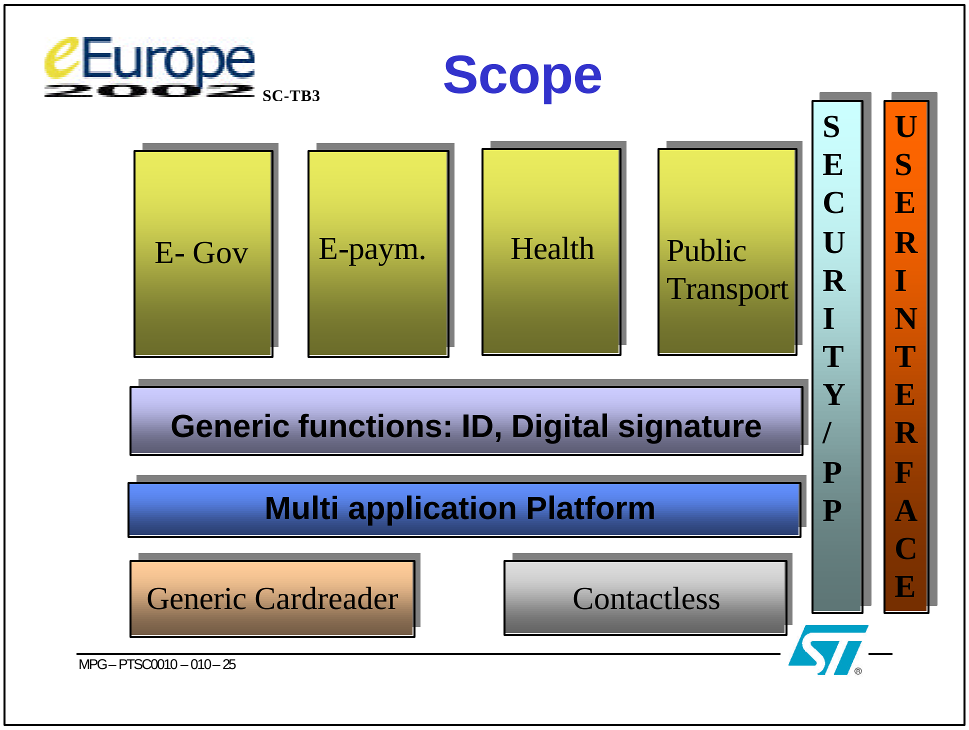
Operating System -- TOE

Hardware -- TOE

Cryptographic Module*

* TOE, TSF, or Environmental Assumption

Source: CygnaCom



eEurope 2002 SC-TB3

Scope

E- Gov

E-paym.

Health

Public Transport

Generic functions: ID, Digital signature

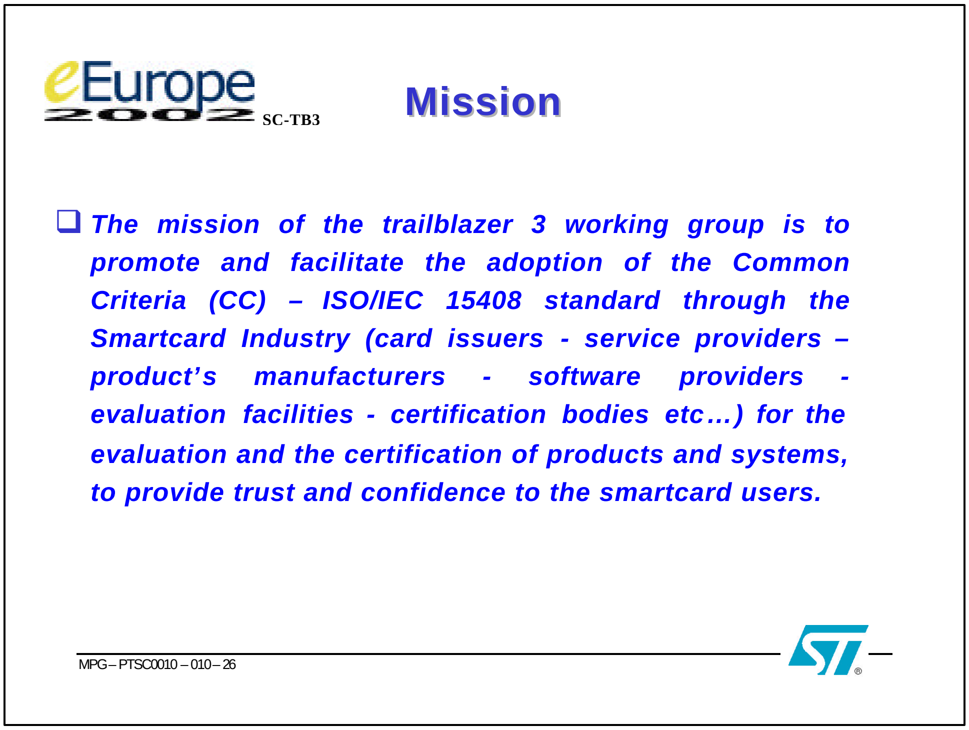
Multi application Platform

Generic Cardreader

Contactless

SECURITY / PP

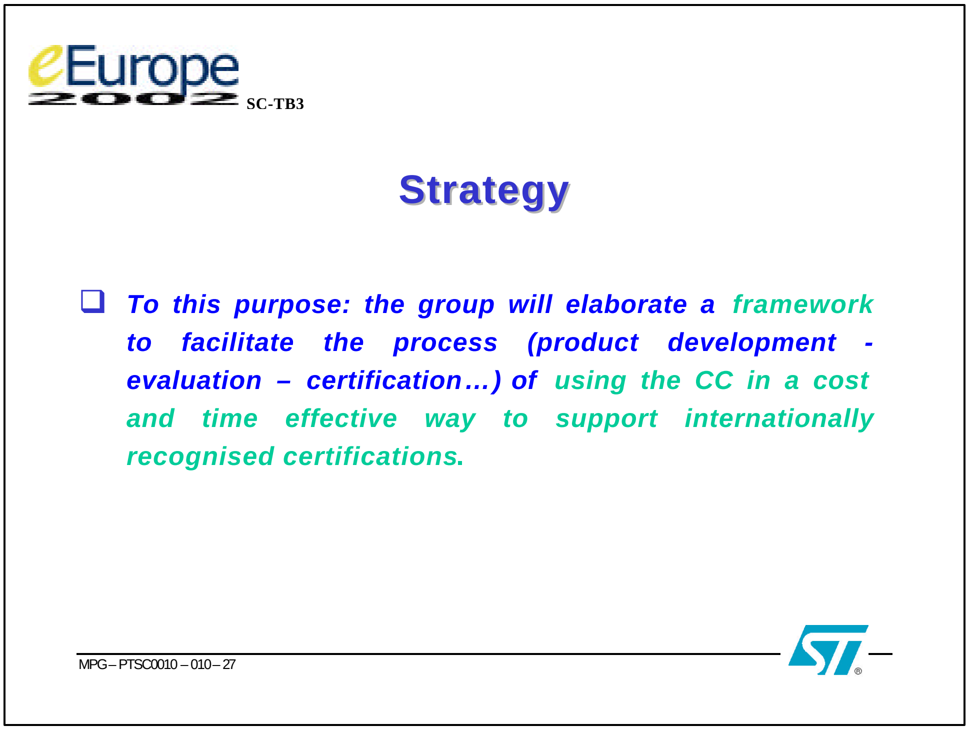
USER INTERFACE



eEurope 2002 SC-TB3

Mission

- ❑ *The mission of the trailblazer 3 working group is to promote and facilitate the adoption of the Common Criteria (CC) – ISO/IEC 15408 standard through the Smartcard Industry (card issuers - service providers – product's manufacturers - software providers - evaluation facilities - certification bodies etc…) for the evaluation and the certification of products and systems, to provide trust and confidence to the smartcard users.*

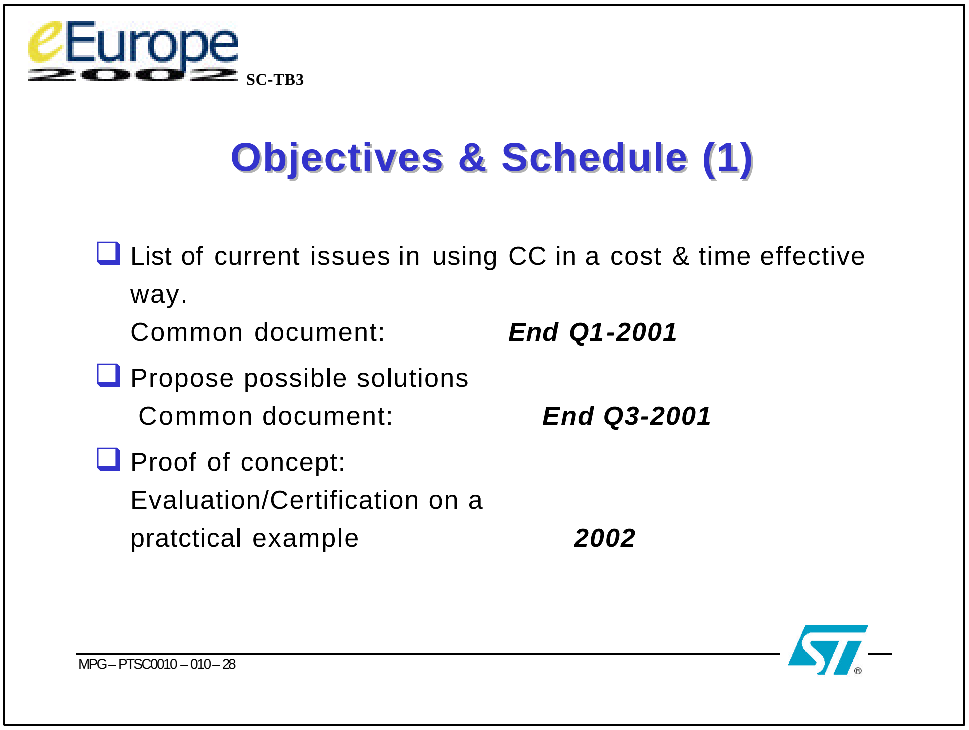


SC-TB3

Strategy

- ❑ ***To this purpose: the group will elaborate a framework to facilitate the process (product development - evaluation – certification…) of using the CC in a cost and time effective way to support internationally recognised certifications.***

MPG – PTSC0010 – 010 – 27

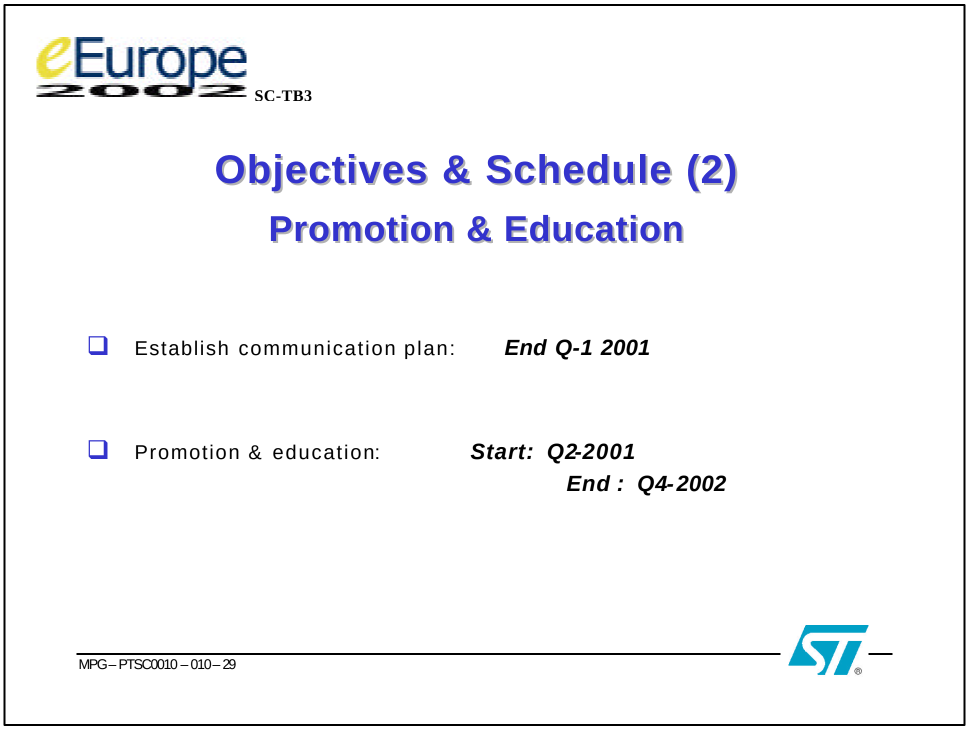


SC-TB3

Objectives & Schedule (1)

- ❑ List of current issues in using CC in a cost & time effective way.
  Common document: ***End Q1-2001***
- ❑ Propose possible solutions
  Common document: ***End Q3-2001***
- ❑ Proof of concept:
  Evaluation/Certification on a
  pratctical example ***2002***

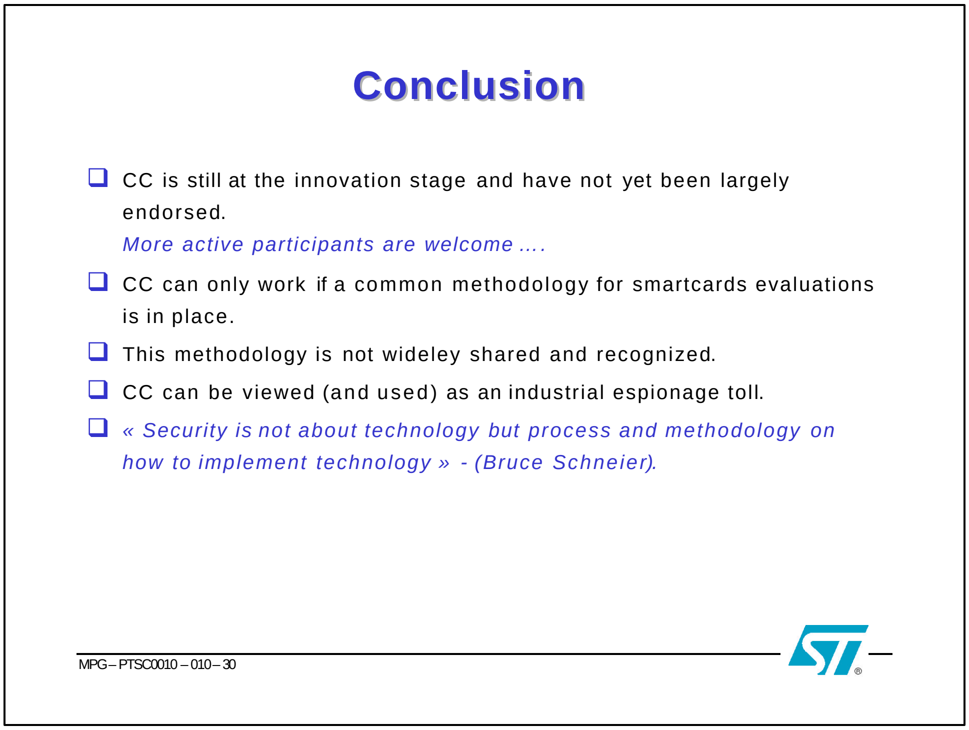
MPG – PTSC0010 – 010 – 28



SC-TB3

Objectives & Schedule (2)
Promotion & Education

- ❑ Establish communication plan: ***End Q-1 2001***
- ❑ Promotion & education: ***Start: Q2-2001***
  End : Q4-2002



Conclusion

- ❑ CC is still at the innovation stage and have not yet been largely endorsed.
  More active participants are welcome ….
- ❑ CC can only work if a common methodology for smartcards evaluations is in place.
- ❑ This methodology is not wideley shared and recognized.
- ❑ CC can be viewed (and used) as an industrial espionage toll.
- ❑ *« Security is not about technology but process and methodology on how to implement technology » - (Bruce Schneier).*