Achievement and good practices from ISCI

Applicable or not to Technical Communities ?

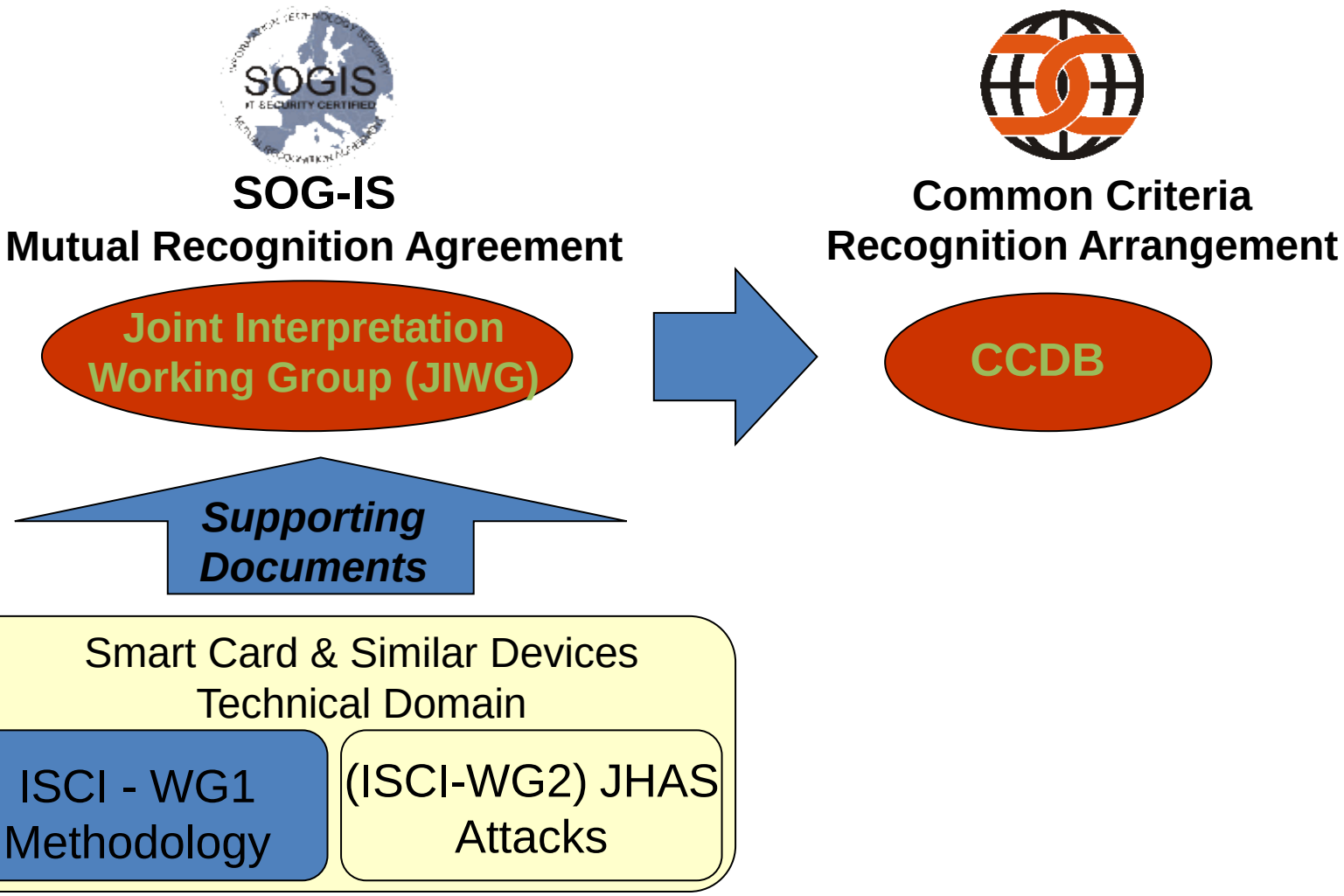
ISCI-WG1 - Eurosmart

Speaker : Francois Guerin

francois.guerin@gemalto.com

ICCC 2013 ORLANDO

ISCI International Security Certification Initiative



ISCI International Security Certification Initiative

ISCI is a **Eurosmart** initiative

Sharing a common objective with JIWG:

Consistent application of the criteria and methods between national schemes

Continuous improvement of the efficiency and cost effectiveness of the process

ISCI WG1 Contributors

IC manufacturers

EM MICROELECTRONIC - Marin SA
A COMPANY OF THE SWATCH GROUP
infineon
inside SECURE
NXP founded by
life.augmented
STARCHIP PRODUCT PROVIDER FOR SEMICONDUCTOR MARKET
Texas Instruments

Smart card manufacturers and issuers

gemalto
Giesecke & Devrient
Oberthur Technologies
SAFRAN Morpho

Evaluation laboratories

Applus
brightsight
cea
leti
SERMA TECHNOLOGIES
SRC security consulting
T · · Systems ·
THALES
TÜViT
Trusted Labs
UL

Certification Authorities

BSI
Bundesamt für Sicherheit in der Informationstechnik
CCN
CESG
Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale
Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

EUROSMART
The Voice of the Smart Security Industry

ISCI WG1 Target

- **Efficient** evaluation & certification process and **consistent** application of them applied **in EU** to **smartcard and similar devices** aiming to reach:
  - high level of CONFIDENCE in product assurance and **resistance**,
  - using EAL4 (or higher) augmented with **AVA_VAN.5** in **unsecure** environment.

ISCI WG1 Context

Increase of

- Product **complexity** and **configurability**,
- Product evaluation scope,
- Product life cycle in the evaluation scope,
- Environment **diversity**,
- **Time to market** pressure
- Development and evaluation **cost** pressure

=> **High creativity to update of rules and practices and constant effort to maintain efficiency**

ISCI WG1 Organization vs TC

- No term of reference
- Equality between members
- Ten year of existence
- Working group leader & subgroup leaders
- Work at subgroup level and share results to complete group to reach consensus
- Definition and promotion of applicable PPs
  (no evaluation method in PP)
- Common understanding and agreement expressed in JIL supporting documents

ISCI WG1 way to proceed

- Shared vision (which direction?)
- Annual objectives & work plan (not only a PP)
- Assess & review priorities
- Focused for major topics

  (topics are often left in progress as not enough strategic)
- Iterative work (regular update of documents aligned on new vision and practices
- Consensus on methods: how to interpret CC?
- Implementation by members keeping the process applicable (TRIAL USE)

Recent ISCI work & achievements

Visible & direct results : JIL supporting documents

Mandatory document to apply for CC evaluation
Security architecture requirements (ADV_ARC) for Smart cards and similar devices
Requirements to perform Integrated Circuit Evaluations

Guidance document to apply for CC evaluation
Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices - Appendix 1

For trial use
Certification of "open" smart card products
Minimum site security requirement

Documents to be published soon:
New PP for Secure IC with code loading (PP BSI-0035 update)
ALC mutualization (see Track XXX)

ISCI WG1 Good Practices to share or not

Sharing and Competition : 4C

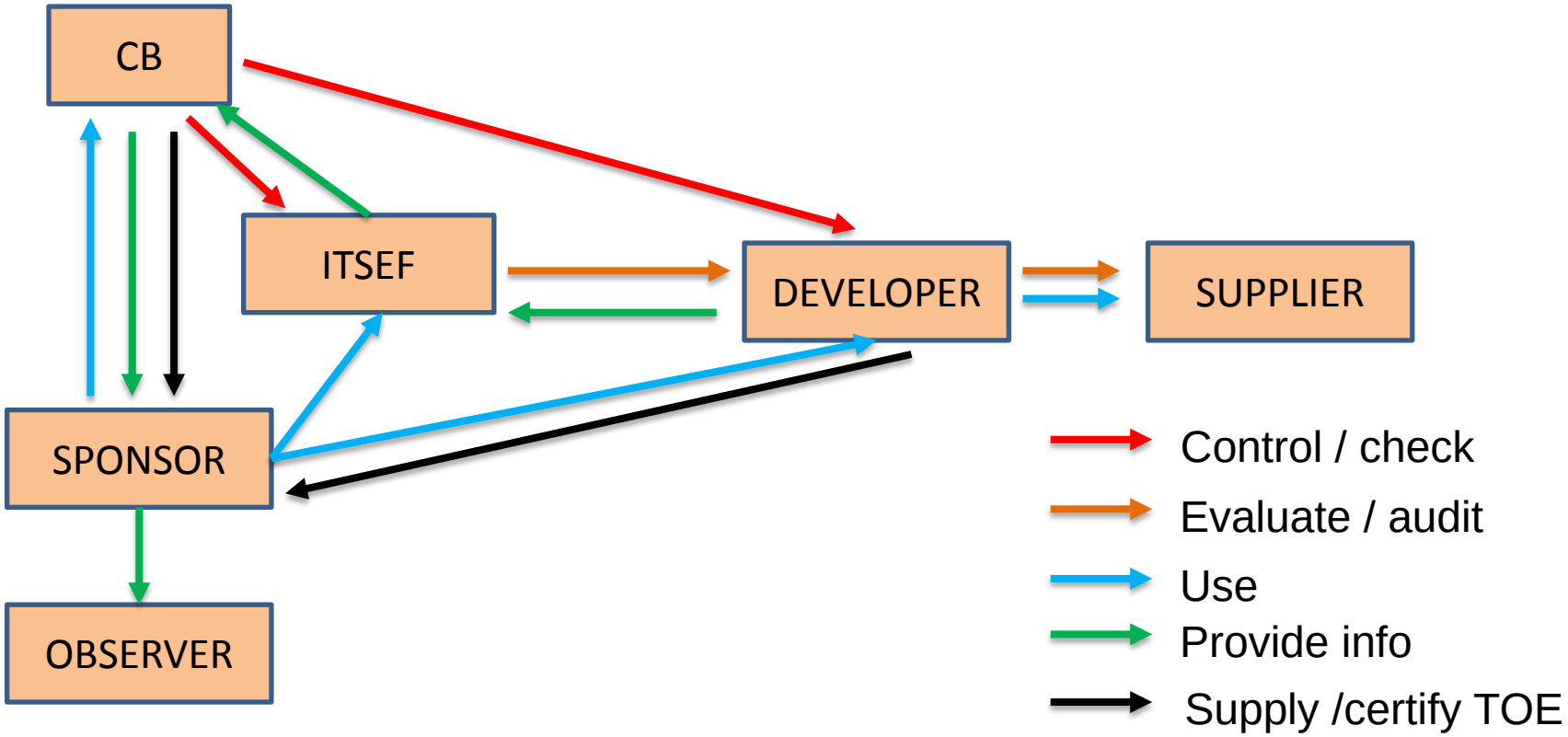
ISCI WG1: organisations but moreover PEOPLE

- **Everyone represents a company, an entity**
- **CONTRIBUTES**
  - bringing ideas, energy, performing work

  on COMMON tasks, participating to same events
- **to create CONFIDENCE and CONSENSUS**
  - obtained by sharing goals, objectives at several levels (Why, What, How, When, How Much)

Do not expect to have deep confidence between several persons without meet them!

Relationship & History



Obtaining confidence inside a TC may differ from actor relationships and common history (1 to 20 years)

Sharing and Competition : Contribute

A simple process to include new member, to motivate contributor (no spy effect)

⇒It requires personal investment and work

⇒It requires coordination and recognition

Issue with logistic at WW level

(work in different time zones, cost of travel)

Size of group & remote management

(time to listen position of members, length of process to obtain consensus not applicable for urgent need)

Sharing and Competition : Common

We define and share vocabulary, common understanding of requirements, rules, evaluation methods and practices, templates **applied to a specific technical domain.**

Start by defining what are the good questions to answer

(eg: definition of properties, mechanism, features, …
what is the real meaning of Trial Use?
what is the sense of unsecure environment?)

Sharing and Competition : Consensus

Consensus requires TIME

(reluctance to change, to adopt new common practices, to take risks, to say we deal with issue probably the same than competitors)

Consensus more easy to obtain with real market pressure on product from Customer

⇒interest to be more efficient on a growing market

Majority vote may be more efficient than consensus for a TC

Reuse & Sharing confidence

Define how to share confidence on evaluation results rather than direct results revealing developer or ITSEF expertise
(limiting transfer of know how between actors)

- See ALC_Mutualization
- See ETR Light
- See Composite evaluation
- See Reuse evaluation

Be clever together : simple & reproductible

- **Make Simple is difficult to achieve**
  - Remain focus on objective : Be efficient
  - Do not try to cover all exceptions
  - Make iteration with Trial use period to assess reproductibility

Collection of evidence is the better example

Minimum Site Requirements increases complexity of audit, but extra confidence allows extension of duration between audits from 1 to 2 years.

Harmonized practices in JIL documents

Writing a JIL document is a long process

– It is interesting only for major topics
– Be aware about selection of topics

– Some topics are left on the road because not enough strategic

– No methodology description in PP because it delays the PP writing and evaluation

CC an efficient tool to share customer confidence

- New vision of CC is application to procurement market

- ISCI vision is Cost of CC evaluation requires to extend CC usage to consumer market driven by private risk managers needing international recognition (payment, PayTv, Telco,…)

- But such market does not follow the same rules.

Conclusion

Objectives of TC and ISCI seem so different

that ISCI good pratices may be not directly applicable.

Good practices have to be adapted with a case by case approach…

Taking in account differences in market needs, tools, culture and practice with wider group of persons and time zone.

THANK YOU FOR YOUR ATTENTION

www.eurosmart.com

For more information …

francois.guerin@gemalto.com