TNO ITSEF BV

A smartcard ST in CC 3.1: what does it look like?

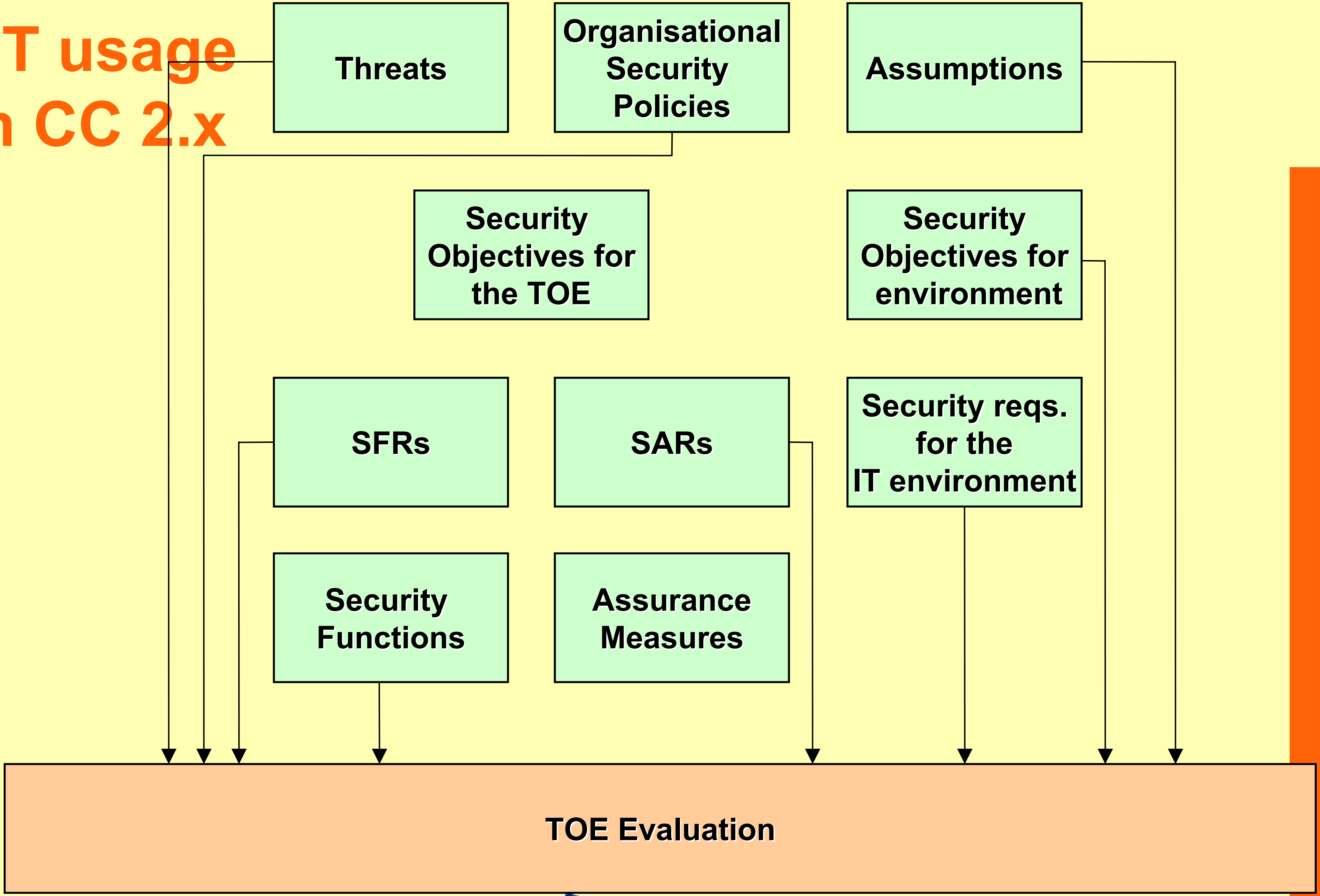
ITSEF BV
Your Partner in Security Approval

Wouter Slegers
+ 31 15 269 2500
slegers@itsef.com
www.itsef.com

Outline of this presentation

- Introduction
- CC semantics change between CC 2.x and 3.x
- What do we want to express?
- How was this done in CC 2.x?
- How can we do this in CC 3.x?
- Conclusion

ST usage in CC 2.x


Threats
Organisational Security Policies
Assumptions
Security Objectives for the TOE
Security Objectives for environment
SFRs
SARs
Security reqs. for the IT environment
Security Functions
Assurance Measures
TOE Evaluation

Resulting CC 2.x semantics

Successful certification means that it is shown to the satisfaction of the Certification Body (via the Evaluation Lab) that:

- The TOE meets the SFRs,
- The TOE protects against the Threats, implements the OSPs
- The TOE implements the Security Functions,

when

- configured according to its guidance, and
- deployed in an environment that meets the objectives for the environment

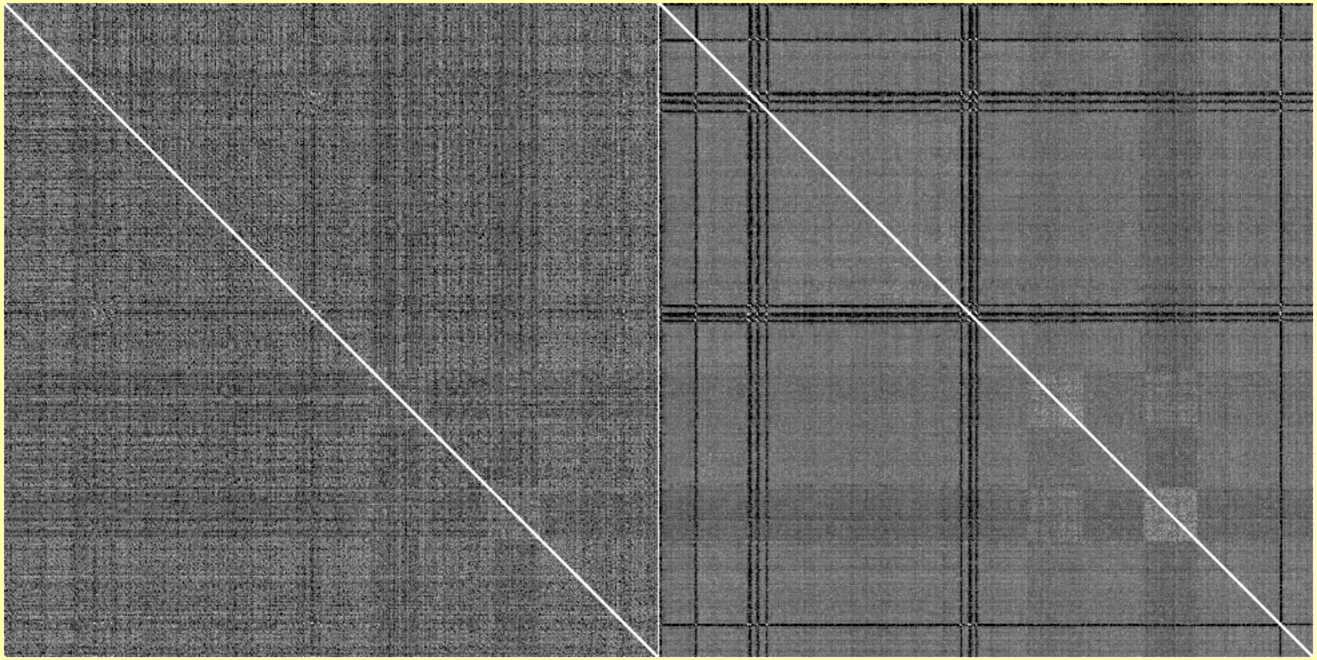
with the limitation that this is

- With the assurance gained from the SARs,
- While ignoring anything that conflicts with the assumptions.

CC 2.x semantics: Example problem situation

Assume in a SF claims timing noise, and this works (left).

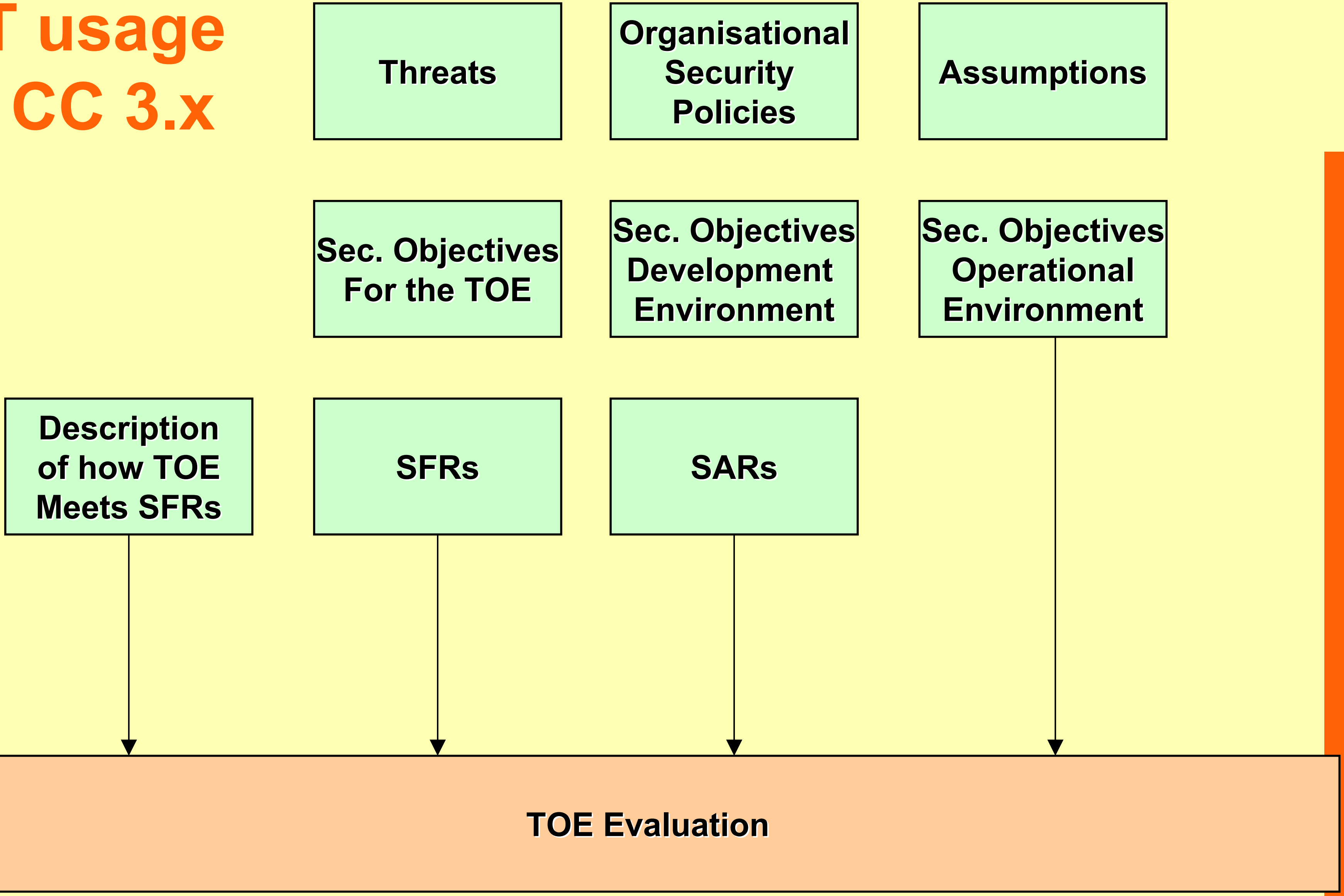
We can disable this timing noise (right), but retrieving the key still was impossible because of the other countermeasures.



Does this fail?

(actual situation occurred in non-CC evaluation)

ST usage in CC 3.x



Threats

Organisational Security Policies

Assumptions

Sec. Objectives For the TOE

Sec. Objectives Development Environment

Sec. Objectives Operational Environment

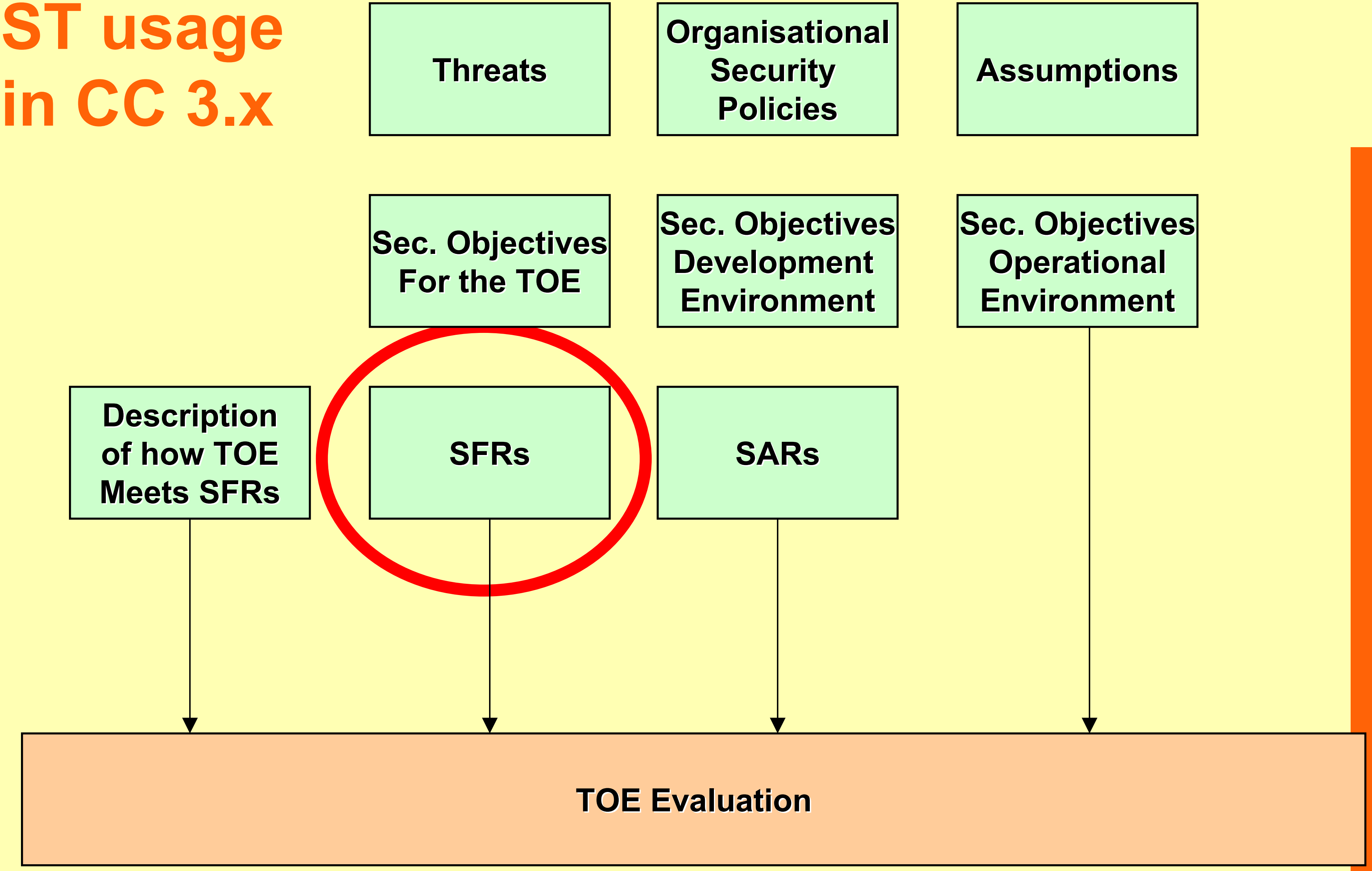
Description of how TOE Meets SFRs

SFRs

SARs

TOE Evaluation

ST usage in CC 3.x


Threats
Organisational Security Policies
Assumptions
Sec. Objectives For the TOE
Sec. Objectives Development Environment
Sec. Objectives Operational Environment
Description of how TOE Meets SFRs
SFRs
SARs
TOE Evaluation

Resulting CC 3.x semantics

Successful certification means that it is shown to the satisfaction of the Certification Body (via the Evaluation Lab) that:

- <u>The TOE meets the SFRs</u>

when

- configured according to its guidance, and
- deployed in an environment that meets the objectives for the environment

with the limitation that this is

- With the assurance gained from the SARs
- While ignoring anything that conflicts with the assumptions.

CC 3.x semantics: impact

It has to be shown that:

- The TOE as delivered to the user,
- In all configurations that are allowed according to the guidance,
- In all environments that fulfill the Objectives for the Environment (as explained in the guidance),

fulfills the assurance measures for all the SFRs.

In particular:

If an attack within the AVA_VLA.x scope breaks even one SFR, the TOE fails evaluation

Meaning of SFRs crucial in CC 3.x:
Example FCS_COP (CC 2.x text):

“FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. “

Typical usage:

The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *DES* and cryptographic key sizes *56bit* that meet the following: *FIPS 46-2*.

Meaning of SFRs crucial in CC 3.x

The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *DES* and cryptographic key sizes *56bit* that meet the following: *FIPS 46-2*.

Breaking that SFR:

- Doing encryption instead of decryption,
- Not correctly executing DES, but not outputting it,
- Not correctly executing DES, outputting that result, allowing DFA on a secret key,
- Doing a 3DES

Not a break of that SFR(?):

- Side channel analysis

Meaning of SFRs crucial in CC 3.x

The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *DES* and cryptographic key sizes *56bit* that meet the following: *FIPS 46-2*.

Breaking that SFR:

- Doing encryption instead of decryption,
- Not correctly executing DES, but not outputting it,
- Not correctly executing DES, outputting that result, allowing DFA on a secret key,
- Doing a 3DES

Not a break of that SFR(?):

- Side channel analysis

Expected meaning

Lets ignore “how to say it” in CC 3.1 for now, what do we want to say?

What does a typical smartcard do? (e.g. What are the business assets?)

- Keep confidentiality of user data
  - ePassport: stored personal information,
  - financial card: transaction data

- Offer operations on the user data (typically only possible after some form of authorization)
  - ePassport: updating of passport information by Issuing State only
  - financial card: calculating payment authorization datagram only after correct PIN entry, at most ATC times,...

What is typically not a business asset?

- Integrity of user data
  - ePassport: covered by environment, e.g. Digital signature on the user data,
  - financial card: typically breaking the integrity of the user data implies breaking the restrictions on the operations

- Confidentiality of parts of the TOE
  - Often mentioned because this is a facilitator for attacks (but this leads to a circular reasoning)
  - Can be policy to implement on smartcard platforms (because it is such a common facilitator for attacks)

Yes, this should trigger discussion at ST writing time, as this is the question, i.e. “What does the TOE claim to provide?”

What does a typical smartcard do? Informal summary:

A smartcard provides the combination of:

- “keeps secrets from the outside world”,

and

- “can do some operation defined on those secrets” (typically under some conditions)

How do we traditionally express this “keeps secrets” in CC 2.x?

In general TOE case, most the Security Targets describe:

- Logical boundary: FPT_SEP
- Physical boundary: FPT_PHP
- Boundary is not bypassable: FPT_RVM

... and do not have operations that break the secrecy.

“Keeps secrets” in CC 2.x for smartcard hardware?

Require boundary with:

- FPT_SEP, FPT_RVM, FPT_PHP

and re-enforce no-leakage over boundary:

- FDP_ITT+FDP_IFC: State that secrets should not leak beyond the boundary when being moved or operated on

Add behavioural boundaries

(matching the way smartcards at that time “kept secrets”):

- FMT_LIM.*: Limit access to test functions and limit the things you can do with the test functions so that confidentiality and integrity user data is not compromised
- FPT_FLT+FPT_FLS: Tolerate extreme conditions and go to “secure state” before they become too extreme

“keeps secrets” in CC 2.x for smartcard products?

Require logical and physical boundary:

- FPT_SEP, FPT_RVM, FPT_PHP,

extend with specific behavioural boundaries:

- FPT_FLS: go to “secure state” before operating conditions become too extreme, or self test fails
- FMT_LIM.*: Limit access to test functions and limit the things you can do with the test functions so that confidentiality and integrity user data is not compromised

And re-enforce with catch-all no boundary crossing:

- FPT_EMSEC: EM-emissions should not emit [assign: emissions] in excess of [assignment: limits] enabling access to passport data.

When do smartcards meet requirement “keeps secrets” in CC 2.x?

The pass/fail criteria hinges on how to interpret

- “secure state”,
- “no substantial information”,
- “enabling access”
- etc, etc,

When do smartcards meet requirement "keeps secrets" in CC 2.x?

The pass/fail criteria hinges on how to interpret

- "secure state",
- "no substantial information",
- "enabling access"
- etc, etc,

so this is <u>interpreted</u>

- With guidance from application notes, and
- Using additional smartcard methodology (ISCI/JIL/JHAS),
- Under ±3 smartcard-experienced certification bodies,
- By ±5 smartcard-expert evaluation labs

Step back, what is happening?

So we express “smartcard TOE can keep secrets”
by officially requiring “smartcard TOE has a boundary”

And somewhere we fudge in the requirements that define:

- how good that boundary has to be exactly, and
- how exactly we are going to test it,
- Etc.

The CCv2.x methodological confusion of checking against Threats, <u>and</u> OSPs, <u>and</u> SFRs <u>and</u> SFs helps:

in the confusion, <u>we choose the “right” one</u>

How about “keep secrets” in CC 3.x?

- FPT_SEP and FPT_RVM removed from part 2,
- “boundary requirement” now part of ADV_ARC
- (FPT_PHP could have been part of this, but is still listed seperately)

Requires evaluator consideration of boundary based on evaluation evidence:

- What boundary is there?
- Why does it protect the TOE from modification?
- Why can’t it be circumvented or penetrated?

How about “keep secrets” in CC 3.x?

- FPT_SEP and FPT_RVM removed from part 2,
- “boundary requirement” now part of ADV_ARC
- (FPT_PHP could have been part of this, but is still listed seperately)

Requires evaluator consideration of boundary based on evaluation evidence:

- What boundary is there?
- Why does it protect the TOE from modification?
- Why can’t it be circumvented or penetrated?

... which is exactly what the smartcard evaluation community already knows how to do.

So “keep secrets” now in ADV_ARC How about “do something”?

Depends on what your smartcard does.

Examples

- Only the administrator can load applications
- Data is only exported after authentication in encrypted form
- The digital signature is calculated after successful authentication by PIN
- The payment authorization datagram is calculated only after succesful authentication, provided that the ATC < ATL, the total spent money < spending limit, ..., during the same session
- ...

Summary

- CC semantics changed between CC 2.x and 3.x
- What we expressed in CC 2.x were SFRs that said “there is a boundary” + “it does something”.
- In CC 3.x “there is a boundary” is part of ADV_ARC.
- The smartcard evaluation community knows in both cases how to interpret this.
- +“It does something” depends on the product.

Questions?

TNO ITSEF BV

Your Partner in Security Approval

Contact information

TNO ITSEF BV
Delftechpark 1
2628 XJ Delft
The Netherlands

Telephone: +31-15-269 2500
FAX: +31-15-269 2555
Email: info@itsef.com
Web: http://www.itsef.com/