brightsight®

your
partner
in security
approval

~~Dirk-Jan Out~~
Wouter Slegers
+ 31 15 269 2500
Slegers@brightsight.com
www.brightsight.com

Further streamlining of PPs and STs

An old hand’s time to kick (out) some new ideas

XXX For internal reference.

Version d.d. 2008-10-19
Author and course maintainer: DJ/Wouter.
Please feed back changes to him.

Biggest changes since N/A:

□ New version

See notes for trainer information

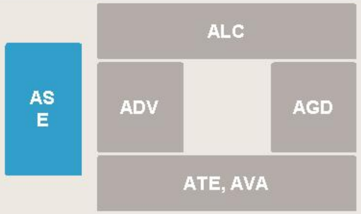
Additional improvements to do:

□ DJ discussie

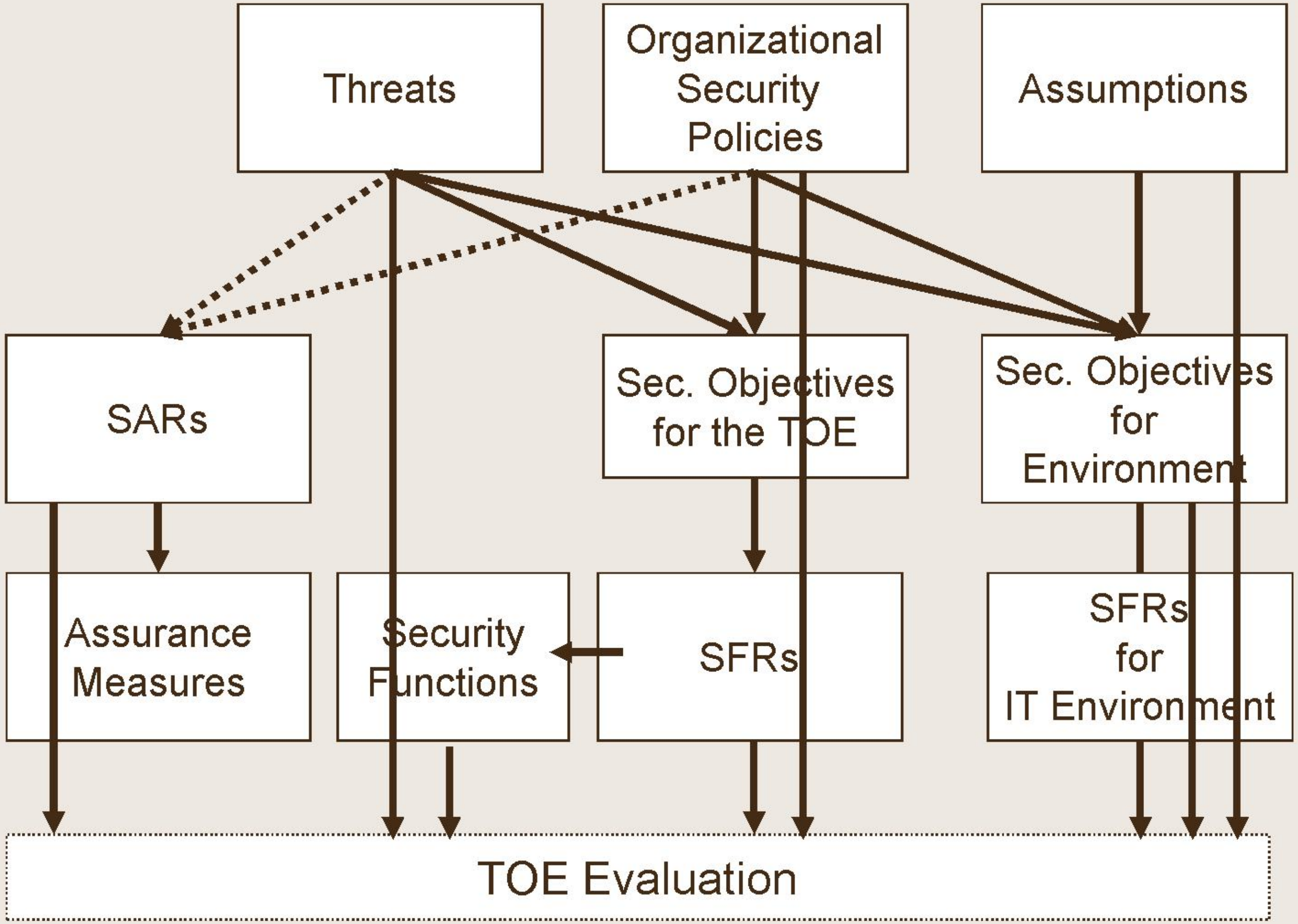
Presentation Targets

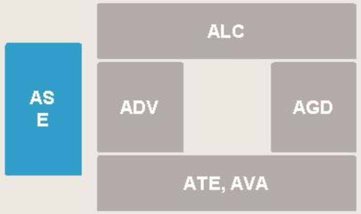
- □ It was not clear what pass/fail for TOE was
- □ SFRs was the answer
- □ SFRs are also not so clear
- □ Now we made a full circle

Unfortunately this presentation is not in the proceedings.
To receive it, email me at slegers@brightsight.com

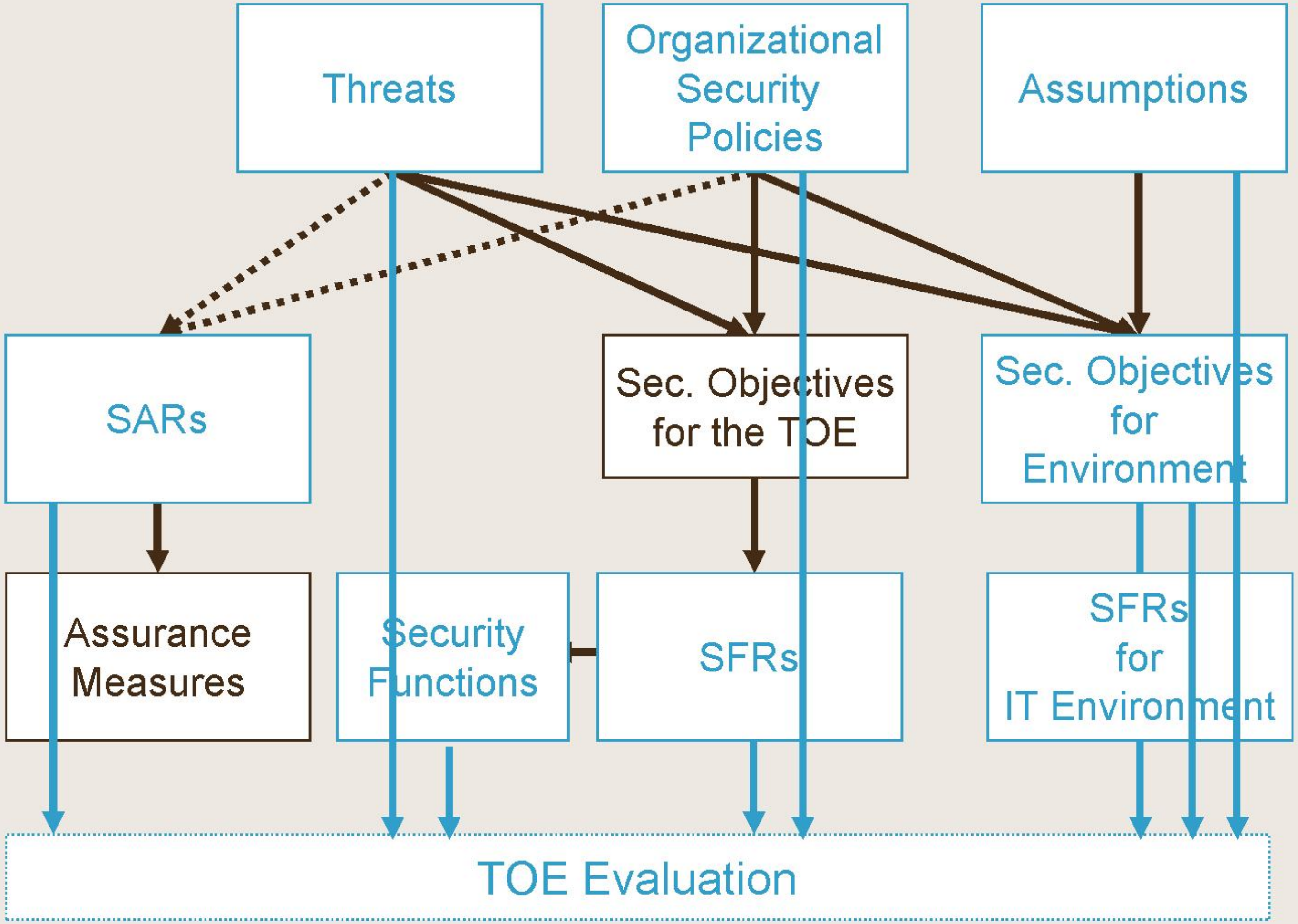


ST structure in CCv2.3





What is used in TOE evaluation in CCv2.3?



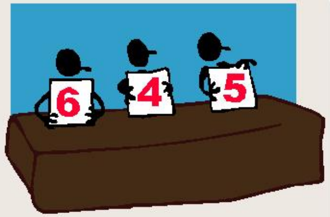
Reason for this:
Definition of 'fail' in CCv2.3?

Threat:	Virus X infects TOE
Objective:	Prevent Virus X from infecting TOE
Requirement:	FPT_SEP.1 (TSF shall protect itself)

The well-known virus Y can destroy the TOE.

Does this fail the evaluation?

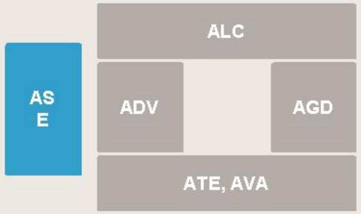
Answers from experienced people



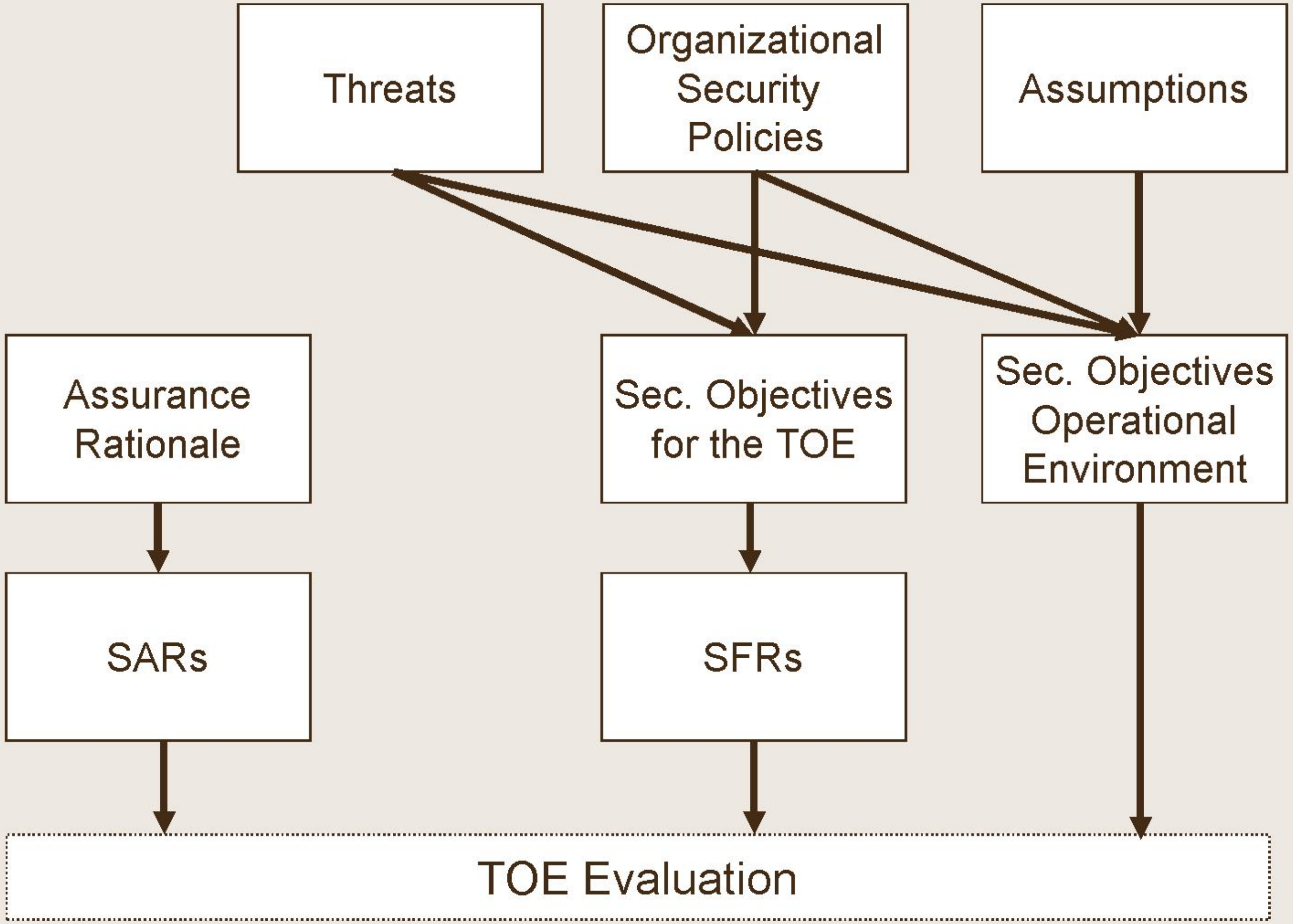
- □ The evaluation fails because the ST is inconsistent
- □ The evaluation fails because FPT_SEP.1 is not met
- □ The evaluation passes, because infection from virus Y is not a threat
- □ The evaluation passes, because it is not a security objective to stop virus Y

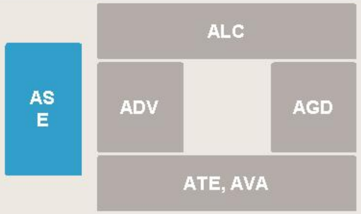
Conclusion:

Fail is being determined based on different parts of the ST (and more)

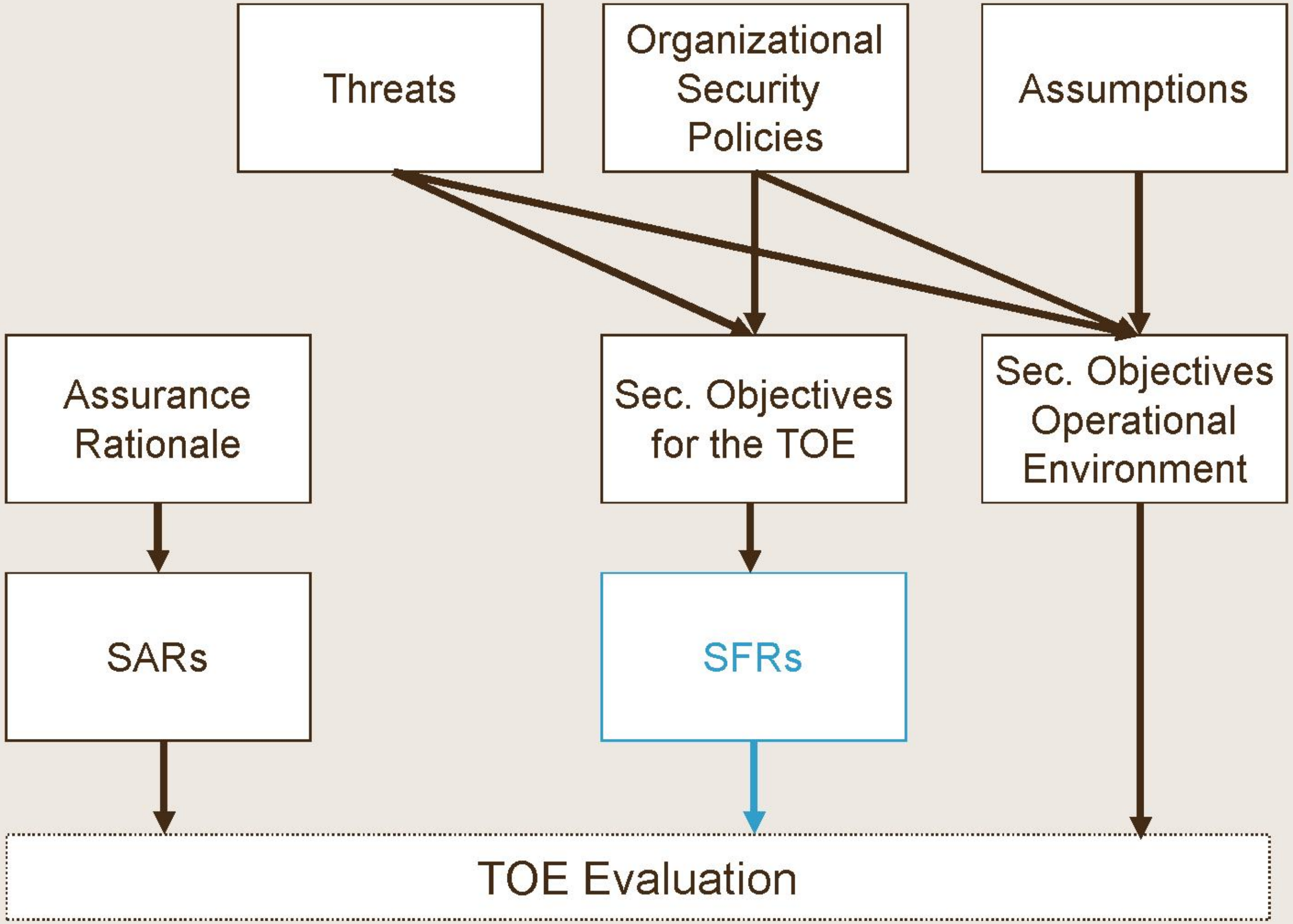


So the PP/ST structure changed to this in CC3.x


Threats
Organizational Security Policies
Assumptions
Assurance Rationale
Sec. Objectives for the TOE
Sec. Objectives Operational Environment
SARs
SFRs
TOE Evaluation



Essential place where pass/fail of TOE is defined


Threats
Organizational Security Policies
Assumptions
Assurance Rationale
Sec. Objectives for the TOE
Sec. Objectives Operational Environment
SARs
SFRs
TOE Evaluation

SFRs are central:
defines pass/fail of evaluation in vulnerability analysis

Attack is succesful and fails the TOE if:

- □ Attacker is in the operational environment
- □ Effort is within Attack Potential
- □ SFR(s) are broken

SFRs are central:
defines pass/fail of evaluation in vulnerability analysis

Attack is succesful and fails the TOE if:

□ Attacker is in the operational environment

□ Effort is within Attack Potential

□ SFR(s) are broken

So how are SFRs used in practice?

Let’s take examples from the PP where we have the most experience with:

The “EuroSmart PP” on IC hardware

(BSI-PP-0002/BSI-PP-0035)

SFRs in use:
Does not express exactly what is needed

FCS_RNG.1.1

The TSF shall provide a physical random number generator that implements total failure test of the random source [assignment: list of additional security capabilities].

FCS_RNG.1.2

The TSF shall provide random numbers that meet [selection: independent bits with Shannon entropy of 7.976 bits per octet, Min-entropy of 7.95 bit per octet, [assignment: other comparable quality metric].

SFRs in use:
Does not express exactly what is needed

FCS_RNG.1.1

The TSF shall provide a physical random number generator that implements total failure test of the random source [assignment: list of additional security capabilities].

FCS_RNG.1.2

The TSF shall provide random numbers that meet [selection: independent bits with Shannon entropy of 7.976 bits per octet, Min-entropy of 7.95 bit per octet, [assignment: other comparable quality metric].

SFRs in use:
Does not express exactly what is needed

Attack:

Drive a nail through chip

- □ Attacker is in the operational environment
  - Yes: smartcards are evaluated with no objectives for the environment when the end-user has them
- □ Effort is within Attack Potential
  - Yes: a hammer, one hit, clearly within even AVA_VAN.1
- □ SFR(s) are broken
  - Yes: The TSF shall provide random numbers

Conclusion: Fail (!?!?)

In practice

Look very hard for a rationale to fit the common understanding

FPT_PHP.3

Application Note 18:

> The Security Target shall describe the automatic response of the TOE. All security functional requirements are defined to protect the User Data stored on the Security IC. Therefore, the security functional requirements are e.g. enforced if the TOE stops operation or does not operate at all if a physical manipulation or physical probing attack is detected.

Verdict: Pass

SFRs in use:
Are also not complete

FDP_ITT.1 Basic internal transfer protection

The TSF shall enforce the Data Processing Policy to prevent the disclosure of user data when it is transmitted between physically-separated parts of the TOE.

FPT_ITT.1 Basic internal TSF data transfer protection

The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE.

FDP_IFC.1 Subset information flow control

The TSF shall enforce the Data Processing Policy on all confidential data when they are processed or transferred by the TOE or by the Security IC Embedded Software.

SFRs in use:
Does not express exactly what is required

Attack:

Read persistent memories when smart card is not powered

- Attacker is in the operational environment
  - Yes: smartcards are evaluated with no objectives for the environment when the end-user has them
- Effort is within Attack Potential
  - Yes (for sake of argument)
- SFR(s) are broken
  - No: The TSF protects during transport and operation

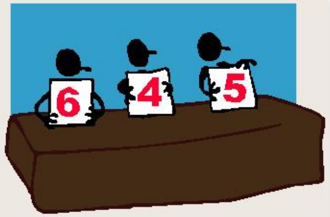
Conclusion: Pass (!?!?)

In practice

The following Security Function Policy (SFP) Data Processing Policy is defined for the requirement “ Subset information flow control (FDP_IFC.1)”:

User Data and TSF data shall not be accessible from the TOE except when the Security IC Embedded Software decides to communicate the User Data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Security IC Embedded Software.

Verdict: Fail



Summary SFRs as decision argument

“A TOE fails if an attack is possible with

- □ Attacker is in the operational environment
- □ Effort is withinin Attack Potential
- □ An SFR(s) are broken”

Leads to situations where

- □ It formally fails (but we pass it), and
- □ It formally passes (but we fail it)

[which shows] how illogical logical thinking can be
Terry Pratchett

We put everything in one egg in one basket, but the egg is broken

The current SFRs are (used in a way) that is

□ Not sufficiently precise

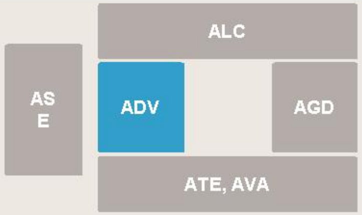
□ Not sufficiently complete

Also

□ SFRs are not orthoganal (there are many ways with different SFRs to express the same requirements)

□ Consistency of SFRs is not at all easy to determine

□ ... And this sofar ignores all further distortion due language / culture / product domain / personal opinions / paper communication / ...



Interpretations to be decided

- □ What does FPT_PHP mean, especially if present?
- □ What do FDP_ITT and FDP_SDI mean, especially if absent?
- □ Does FCS_COP imply DPA/DFA mechanisms need to be in ADV_ARC?
- □ FCS_RND imply AIS20/31 requirements?

Interpretation by TOE-type the way to go (smartcards: JIL/ISCI)

What to do with this problem?

- Ignore the problem
  - Do nothing
  - Make small changes to CC Part 2
- Change something to fix the problem
  - New SFRs (CC 3.0)
  - Going to SFRs only was a mistake: bring back Security Functions
  - Going to SFRs was a mistake: use Objectives for the TOE
  - Make a new language...
- Acknowledge the problem, seek the solutions elsewhere
  - Accept the differences
  - Create community surrounding a PP to align interpretations

What to do with this problem?

- Ignore the problem
  - Do nothing
  - Make small changes to CC Part 2
- Change something to fix the problem
  - New SFRs (CC 3.0)
  - Going to SFRs only was a mistake: bring back Security Functions
  - Going to SFRs was a mistake: use Objectives for the TOE
  - Make a new language...
- Acknowledge the problem, seek the solutions elsewhere
  - Accept the differences
  - Create community surrounding a PP to align interpretations

New SFRs (or any other language) is not going to work…

An old hand’s time to kick

- CC 3.0 trial of new SFRs
- Package was designed to strongly encourage:
  - Precise requirements
  - Only necessary requirements
  - Split of requirements in
    - What the TOE does internally
    - What the TOE does in interaction to the outside world
  - Avoidance of technology / solution specific requirements

New SFRs (or any other language) is not going to work…

An old hand's time to kick

- CC 3.0 trial of new SFRs
- Package was designed to strongly encourage:
  - Precise requirements
  - Only necessary requirements
  - Split of requirements in
    - What the TOE does internally
    - What the TOE does in interaction to the outside world
  - Avoidance of technology / solution specific requirements
- SFR-language was
  - Concise
  - Orthaganal
  - Abstract
  - I.e. Logic-language like

New SFRs (or any other language) is not going to work…

An old hand's time to kick

Reasons not to adapt (as seen by the author):

- □ Some constructs previously possible, now not possible
- □ Some constructs previously not possible, now also not possible
- □ Some constructs require more SFRs
- □ It is too abstract
- □ …

It was too big a change

To make an omelet without breaking an egg…

Any real solution to this in the Common Criteria will require big changes to the SFRs (or whatever language replaces it)

+

Big changes are not acceptable

=

No real solution to this is viable

What to do with this problem?

- Ignore the problem
  - Do nothing
  - Make small changes to CC Part 2
- Change something to fix the problem
  - New SFRs (CC 3.0)
  - Going to SFRs only was a mistake: bring back Security Functions
  - Going to SFRs was a mistake: use Objectives for the TOE
  - Make a new language...
- Acknowledge the problem, seek the solutions elsewhere
  - Accept the differences
  - Create community surrounding a PP to align interpretations

Solution direction

> First there was nothing.
> And God said: “Let there be light”, and there was light
> and there still was nothing, but at least you could see it
> Terry Pratchett

- Accept that the SFRs are not the stand-alone truth
- Seek solution in interpretation, choose between:
  - Accept that there are interpretation differences

    or

  - Create and maintain consensus interpretation

Solution direction

> First there was nothing.
> And God said: “Let there be light”, and there was light
> and there still was nothing, but at least you could see it
> Terry Pratchett

- Accept that the SFRs are not the stand-alone truth
- Seek solution in interpretation, choose between:
  - Accept that there are interpretation differences

    or

  - Create and maintain consensus interpretation

Create and maintain consensus on interpretation

- Gather stakeholders
  - Users
  - Developers
  - Evaluators
  - Certifiers
- Discuss, compare, improve, align, make (mandatory) guidance....

Further streamlining of PPs and STs

Create and maintain consensus on interpretation
Example: smart card community with EuroSmart, ISCI,…

- Gather stakeholders
  - Users: gemalto, Giesecke & Devrient, Oberthur Card Systems, Sagem Orga SAFRAN Group, Trusted Labs
  - Developers: ATMEL, infineon, NXP, RENESAS Everywhere you imagine., ST, GROUPEMENT DES CARTES BANCAIRES "CB"
  - Evaluators: leti, SERMA TECHNOLOGIES, T-Systems, brightsight® your partner in security approval
  - Certifiers: BSI Bundesamt für Sicherheit in der Informationstechnik, CCN, Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE Premier ministre Secrétariat général de la défense nationale, TNO

- Discuss, compare, improve, align, make (mandatory) guidance….

  CDDB-2006-06-001, CCDB-2006-04-001, CCDB-2008-04-001, CCDB-2006-04-003, CCDB-2007-09-01, CCDB-2007-09-02, CCDB-2006-04-004, CCDB-2006-04-007

Summary

□ It was not clear what pass/fail for TOE was

□ SFRs was the answer

□ SFRs are also not so clear

□ Now we made a full circle

Questions?

Contact information

Note: the name “TNO ITSEF” has changed to “Brightsight”

Brightsight BV
Delftechpark 1
2628 XJ Delft
The Netherlands

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