brightsight®

your
partner
in security
approval

Wouter Slegers
+ 31 15 269 2500
Slegers@brightsight.com
www.brightsight.com

The complete(d) CC v3.1 experience on a smart card IC with cryptolibrary

Or: CC works for smartcards
as good as ever

XXX For internal reference.

Version d.d. 2008-09-01
Author and course maintainer: Wouter.
Please feed back changes to him.

Biggest changes since N/A:

- □ New version

See notes for trainer information

Additional improvements to do:

- □ Cost analysis (vs CAST-like evaluations)

Presentation Targets

Describe our final experiences with CCv3.1 Release 1 on a smartcard IC

- CC v3.1 evaluation of smart cards
  - ST
  - Security Architecture
- Training of CC v3.1 to evaluators
- Usefulness of CC

This was made possible by:

Developer and Sponsor:

TOSHIBA
Leading Innovation >>>

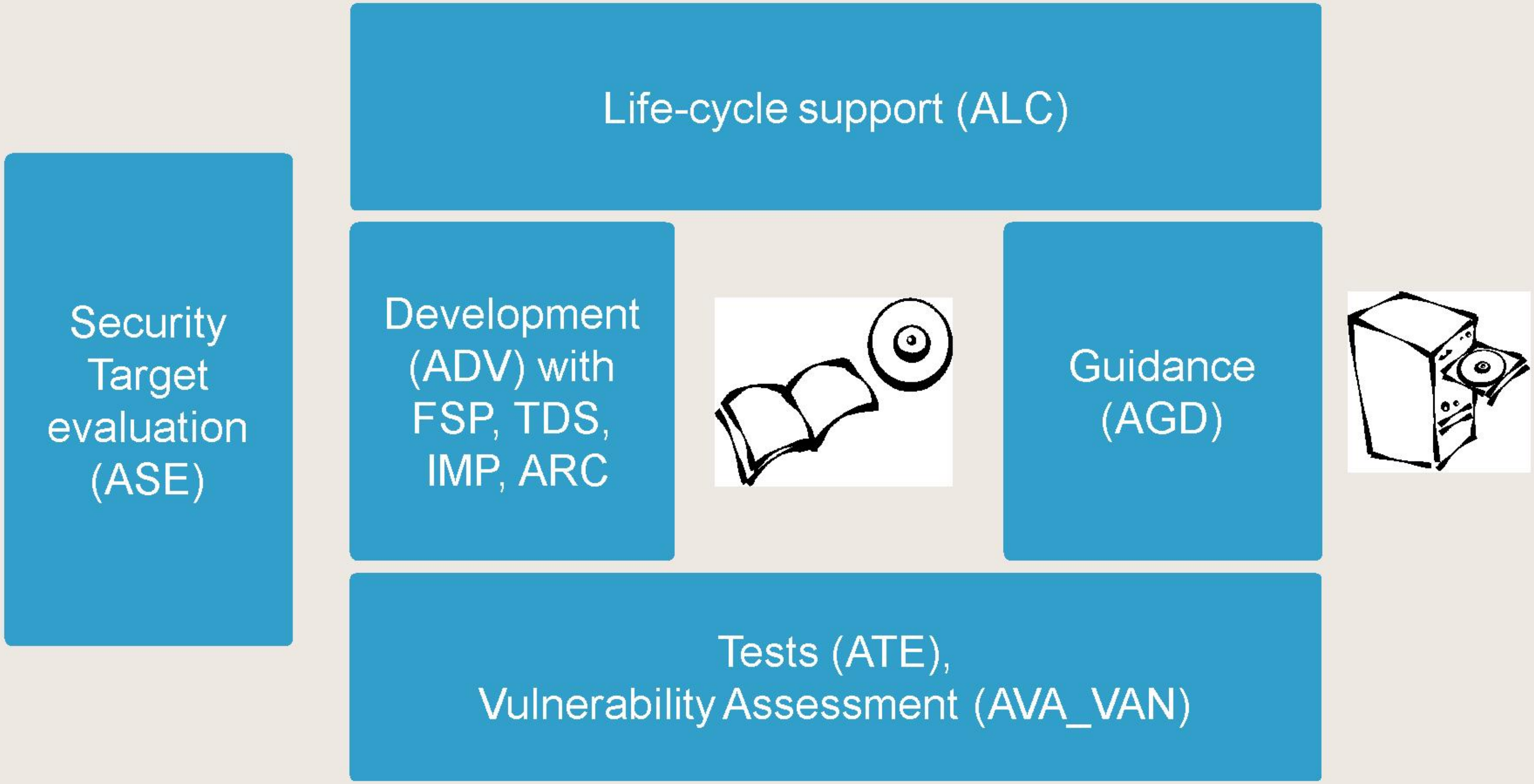
Certification Body:

CERTIFICATION TNO

Netherlands Scheme for Certification in the area of IT Security (NSCIB)

As usual, this presentation is my opinion,
I do not speak for others.

Common Criteria in one slide



Life-cycle support (ALC)

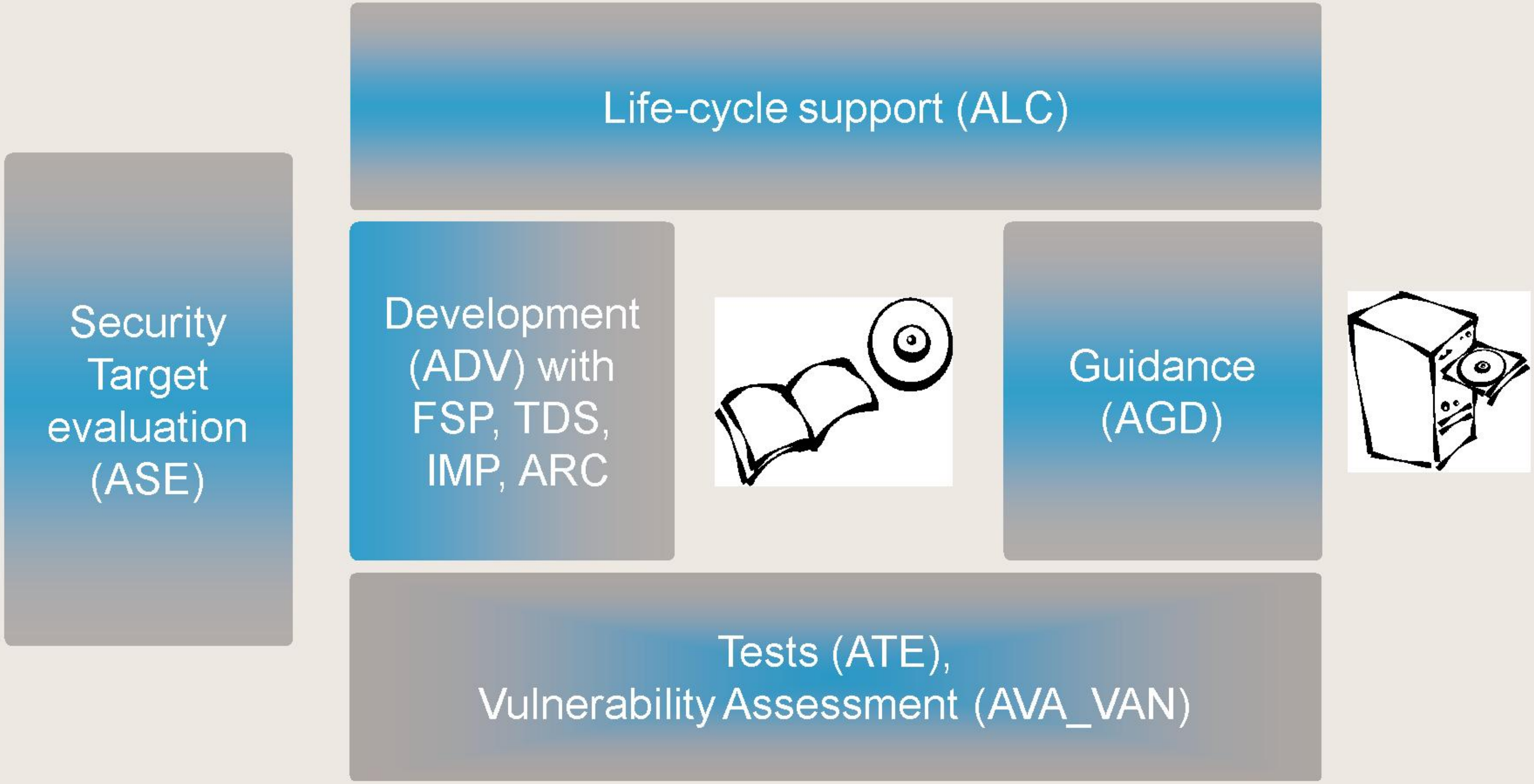
Security Target evaluation (ASE)

Development (ADV) with FSP, TDS, IMP, ARC

Guidance (AGD)

Tests (ATE),
Vulnerability Assessment (AVA_VAN)

Impact to the paperwork



Life-cycle support (ALC)

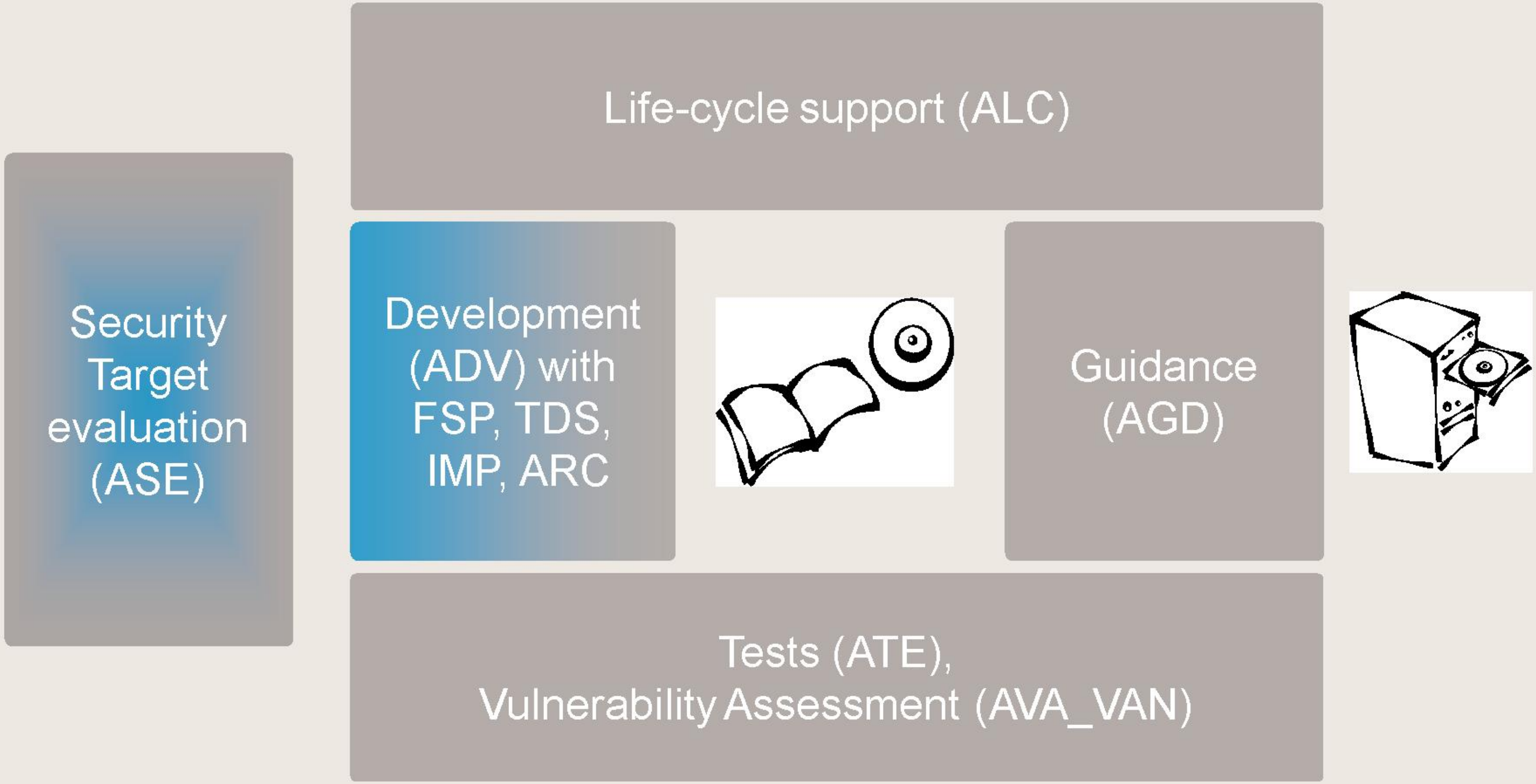
Security Target evaluation (ASE)

Development (ADV) with FSP, TDS, IMP, ARC

Guidance (AGD)

Tests (ATE),
Vulnerability Assessment (AVA_VAN)

Content wise changes



Life-cycle support (ALC)

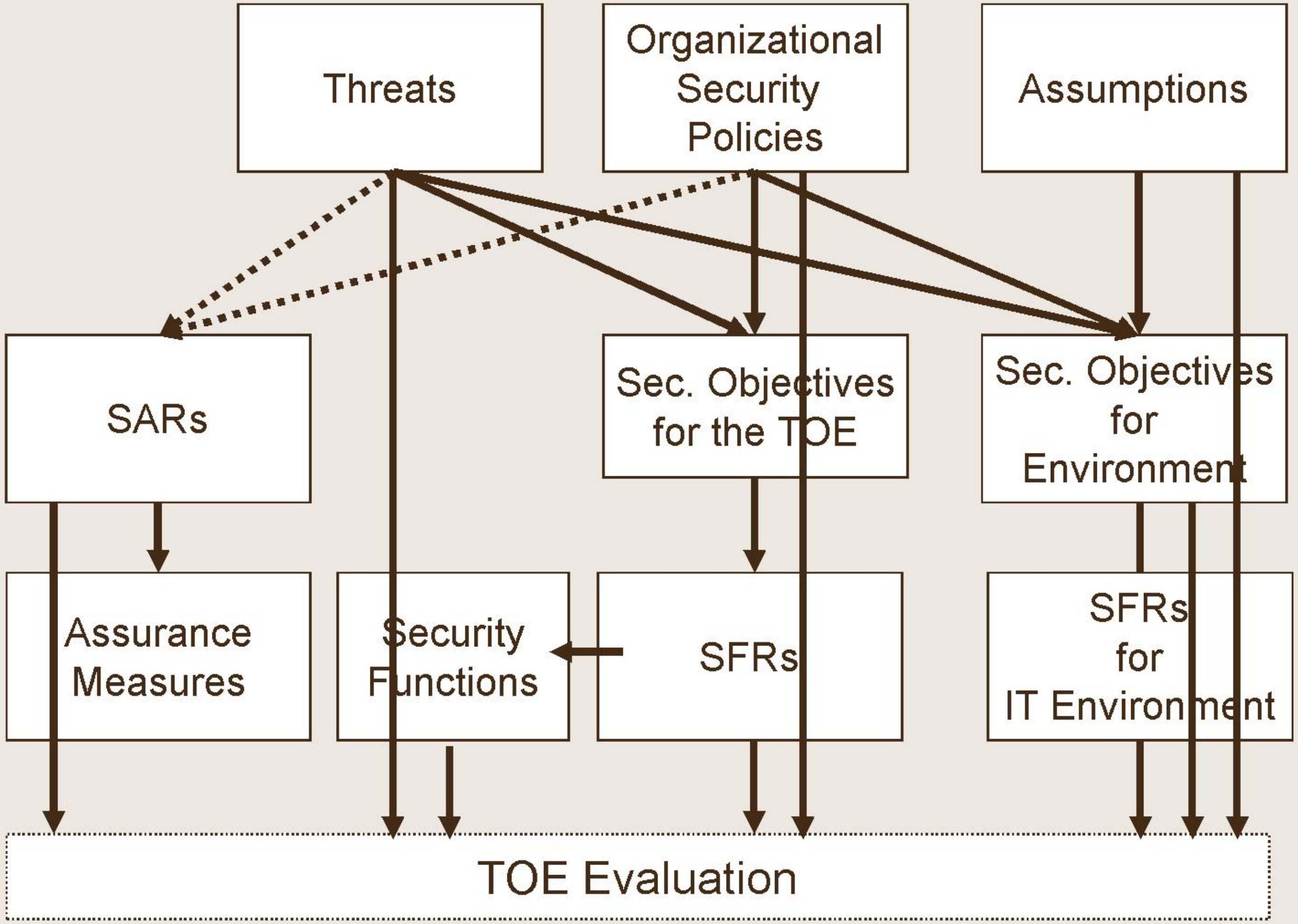
Security Target evaluation (ASE)

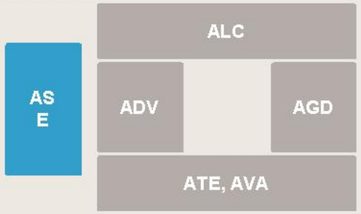
Development (ADV) with FSP, TDS, IMP, ARC

Guidance (AGD)

Tests (ATE),
Vulnerability Assessment (AVA_VAN)

ST structure went from this…





ASE

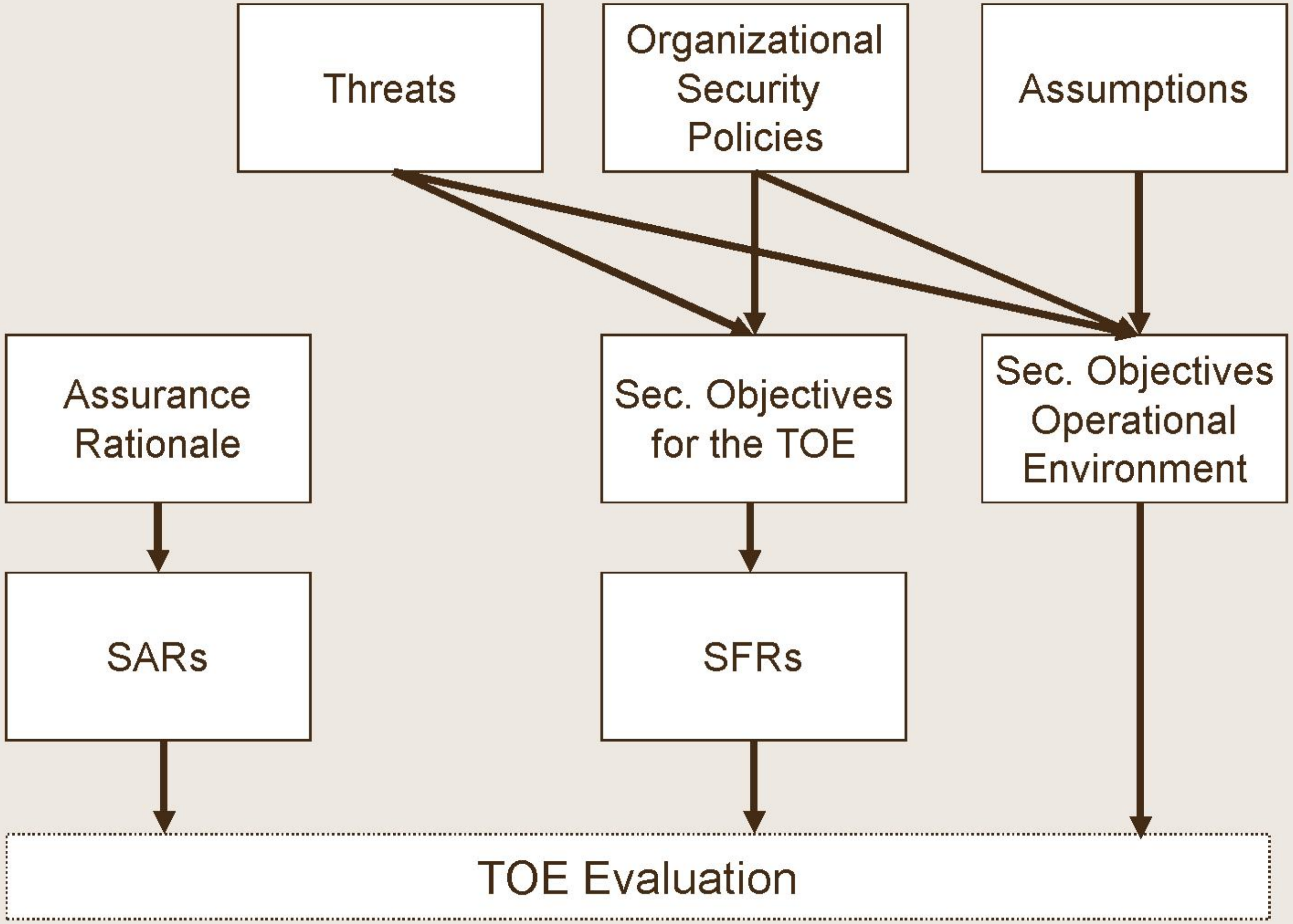
ALC

ADV

AGD

ATE, AVA

… to this



Threats

Organizational Security Policies

Assumptions

Assurance Rationale

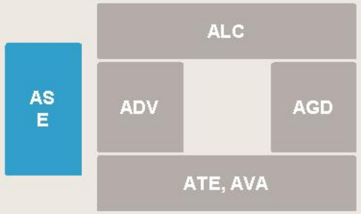
Sec. Objectives for the TOE

Sec. Objectives Operational Environment

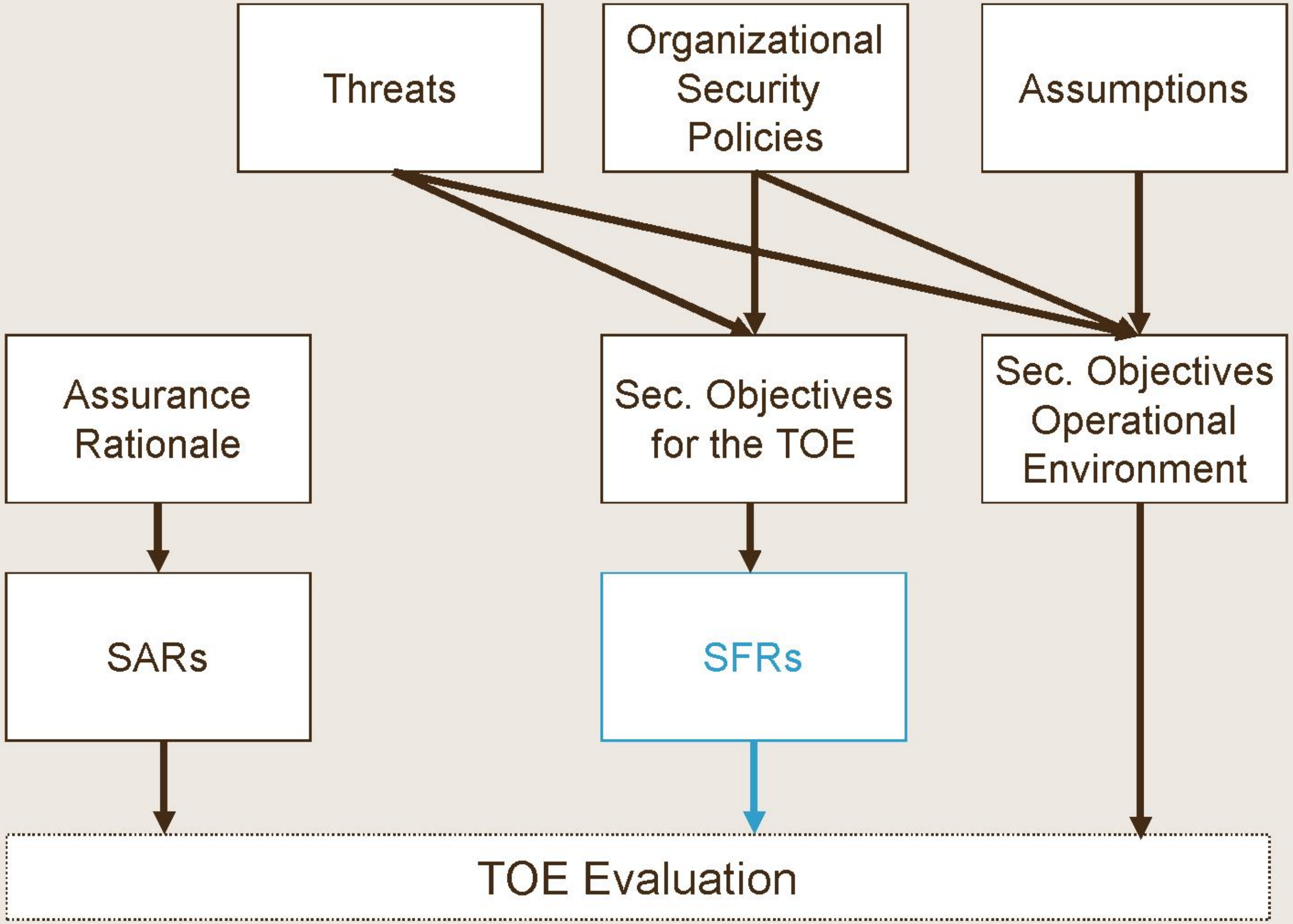
SARs

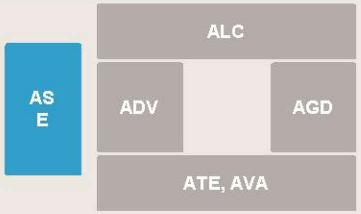
SFRs

TOE Evaluation



Essential change


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



Experience ST changes

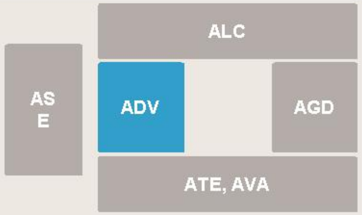
CCv2.x structure and result:

- Tracing SFRs and Security Functions
- What the TOE does
- What requirements are to be met

CCv3.x structure and result:

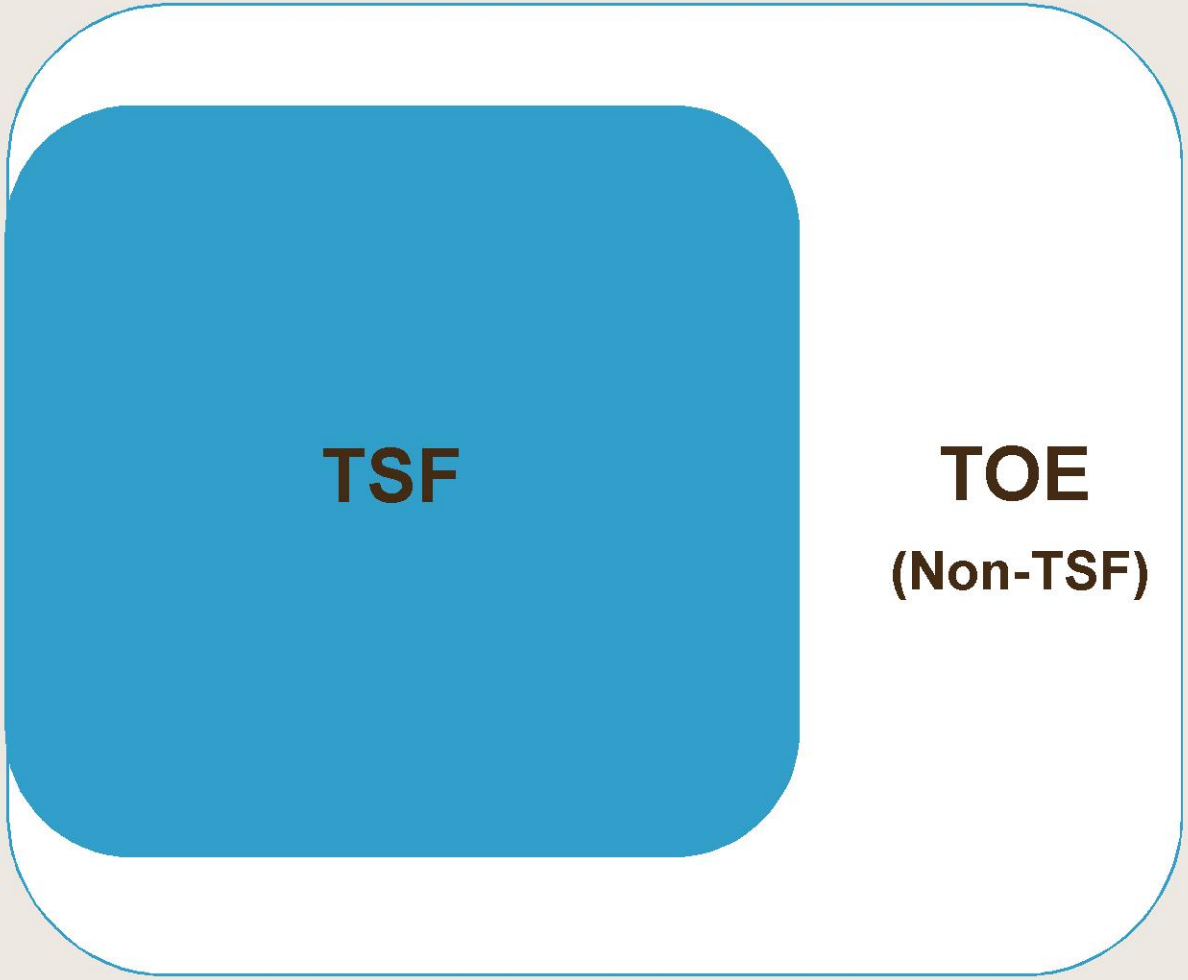
- Tracing the SFRs
- Describe how the TOE is meeting the requirements

SFR-centrality is good & bad
(see presentation Dirk-Jan Out)



ADV describes the TOE

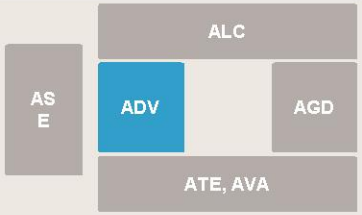
ADV_TDS and lower splits TOE in TSF and “the other part” (Non-TSF)



TSF

TOE

(Non-TSF)



ALC

AS
E

ADV

AGD

ATE, AVA

ADV_FSP/TDS introduces explicit labeling

Labelling:

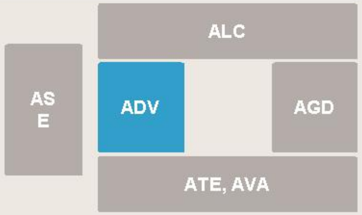
- SFR-enforcing
  - Directly implements a SFRs

- SFR-supporting
  - If this part misbehaves, a SFR is no longer fulfilled

- SFR-non-interfering
  - If this part is hostile, it can influence a SFR.

- None of the above: TOE but not TSF (non-TSF)

ADV_FSP/TDS introduces explicit labeling



Labelling:

- SFR-enforcing
  - Directly implements a SFRs
- SFR-supporting
  - If this part misbehaves, a SFR is no longer fulfilled
- SFR-non-interfering
  - If this part is hostile, it can influence a SFR.
- None of the above: TOE but not TSF (non-TSF)

TOE

Label defines minimum of TSF

Labelling:

- SFR-enforcing
  - Directly implements a SFRs
- SFR-supporting
  - If this part misbehaves, a SFR is no longer fulfilled
- SFR-non-interfering
  - If this part is hostile, it can influence a SFR.

TSF

- None of the above: TOE but not TSF (non-TSF)

Critical test:
can it influence a SFR?

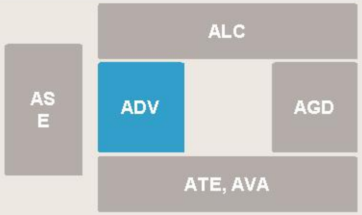
Labelling:

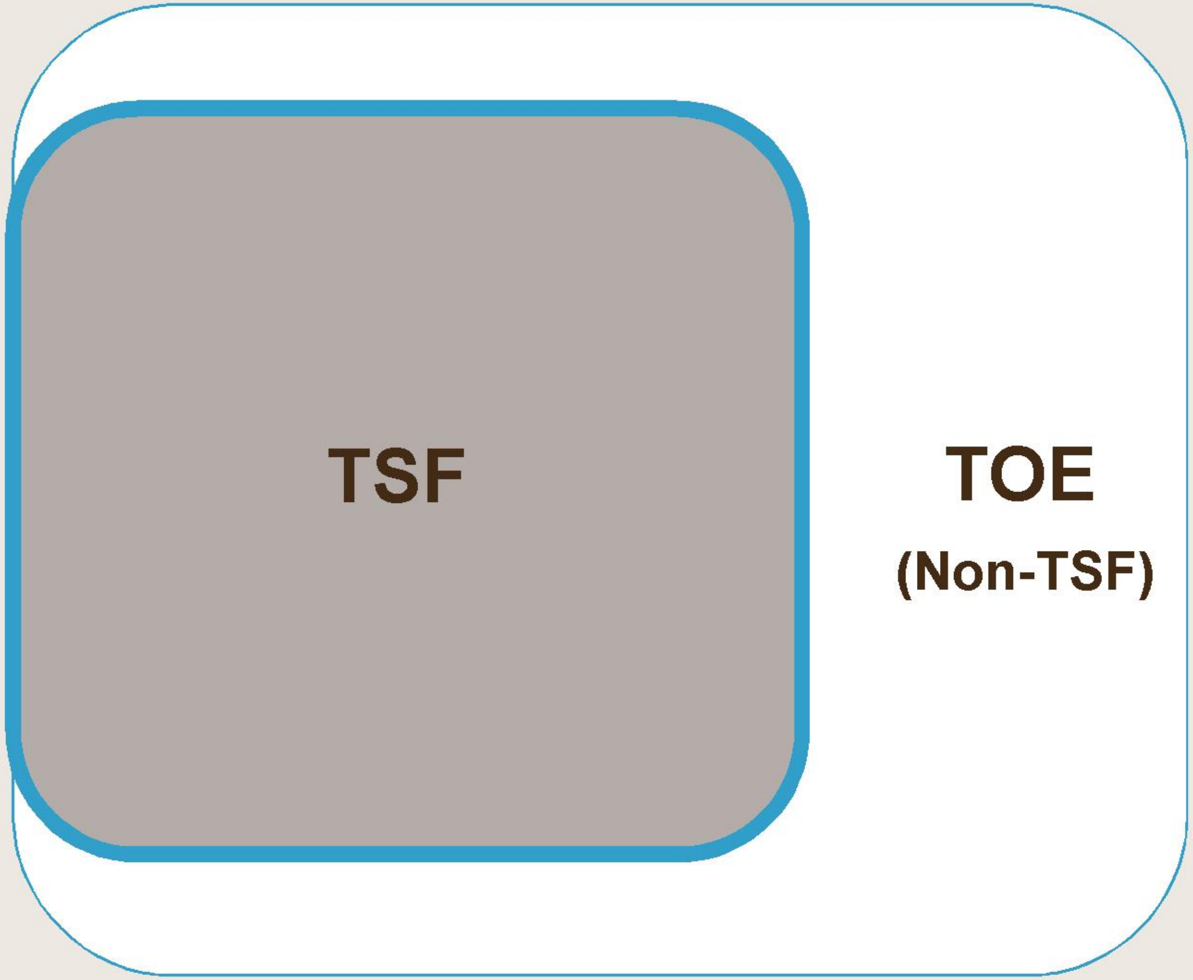
TSF

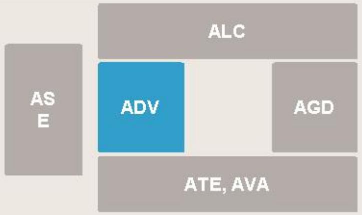
- □ SFR-enforcing
  - Directly implements a SFRs
- □ SFR-supporting
  - If this part misbehaves, a SFR is no longer fulfilled
- □ SFR-non-interfering
  - If this part is hostile, it can influence a SFR.

- □ None of the above: TOE but not TSF (non-TSF)

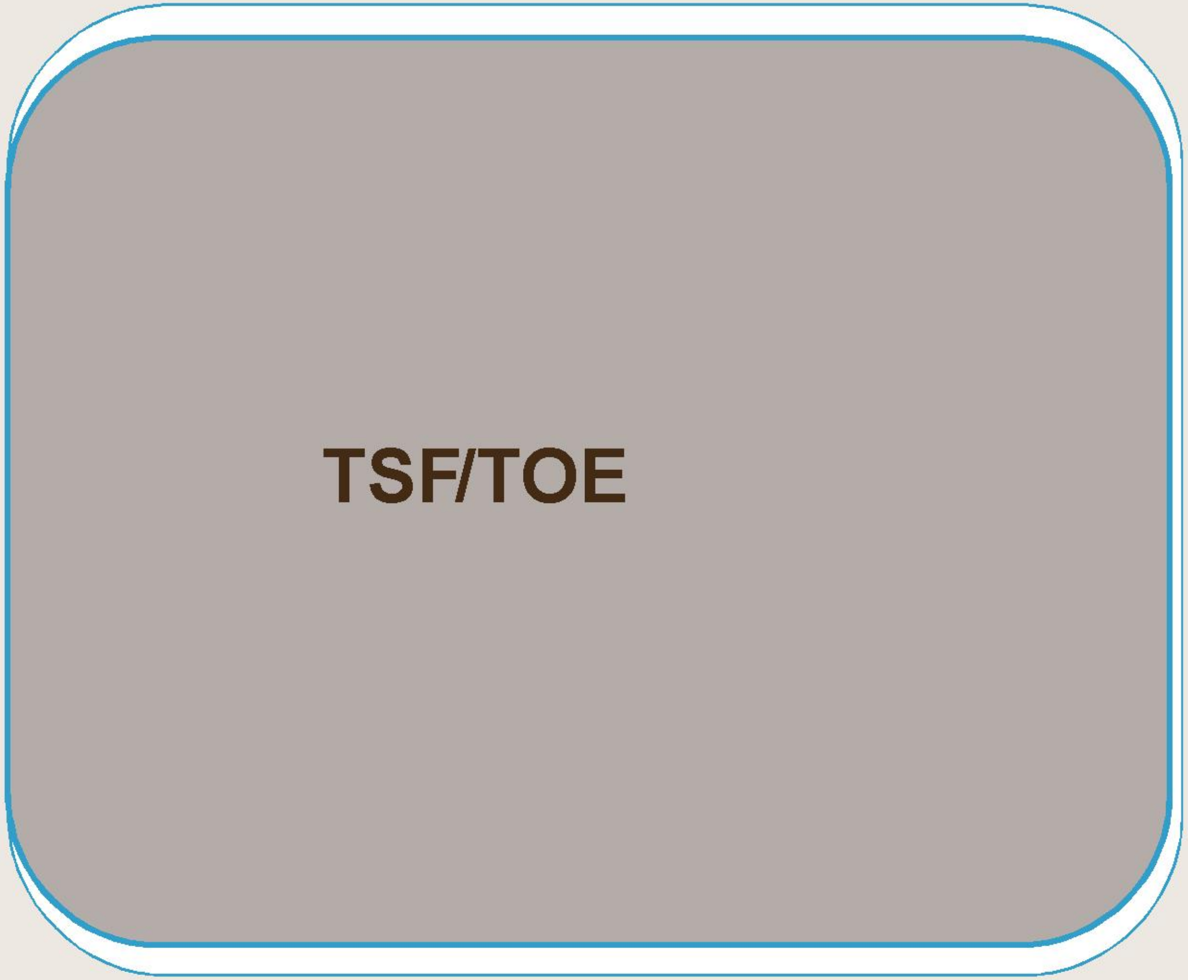
Security Architecture (ADV_ARC) describes what protects the TSF

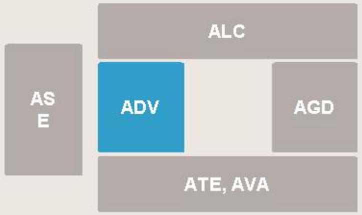




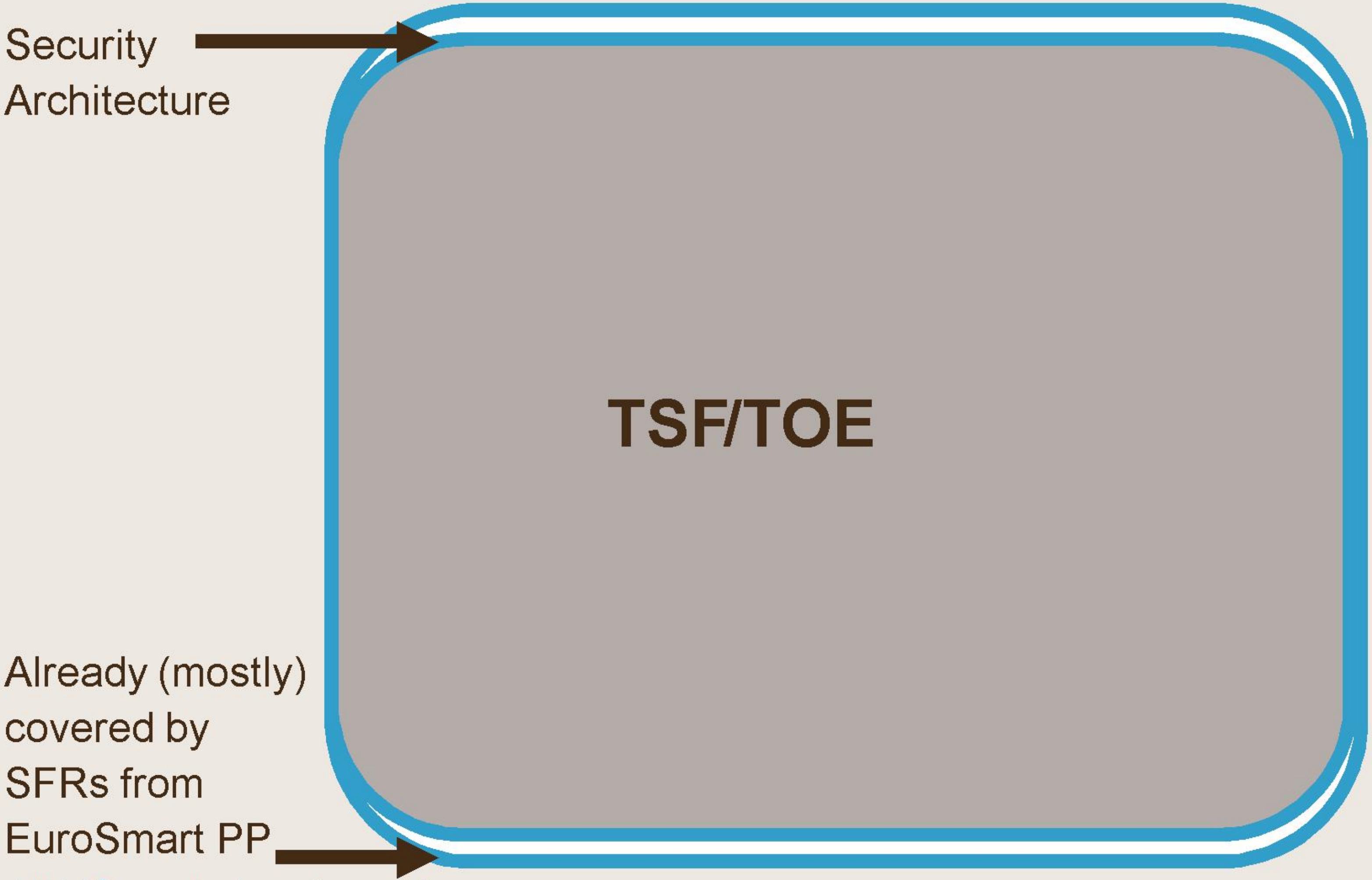


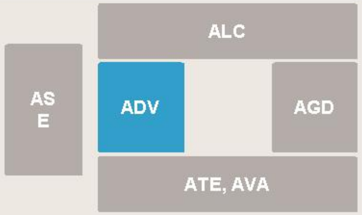
In smartcard hardware case:
TOE ~= TSF





In smartcard hardware case: TOE ~= TSF





ALC

ASE

ADV

AGD

ATE, AVA

ADV_ARC for smartcards

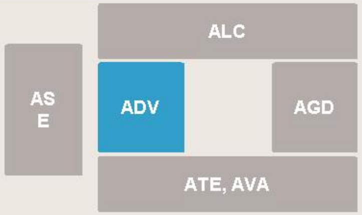
First confused question:

- How is it different from the SFRs that already describe self protection?

Answer (for smartcard ICs):

- It is not (really) different

Summary of evaluation impact



The good:

- ST evaluations have become easier
- Design has become a bit easier
  - Only tracing of SFRs, only one way
- Lifecycle work has been collapsed to reduce duplicity
- The SFRs are central

The bad:

- Not much has changed
- No real work reduction

The ugly:

- The SFRs are central (See Dirk-Jan Out's talk)

Presentation Targets

Describe our final experiences with CCv3.1 Release 1 on a smartcard IC

- CC v3.1 evaluation of smart cards
  - ST
  - Security Architecture
- Training of CC v3.1 to evaluators
- Usefulness of CC

Training of CC v3.1 to evaluators

Background:

- Brightsight had strong involvement in CC3.x
  - Quite some internal discussion
  - Internal presentations ongoing process etc.
- Many evaluators already CC2.x trained & experienced
- Internal methodology already updated to CC3.x

Still, evaluators need training:

- To perform evaluation tasks efficiently
- To perform evaluation correctly, and
- To meet formal accreditation requirements

Training of CC v3.1 to evaluators

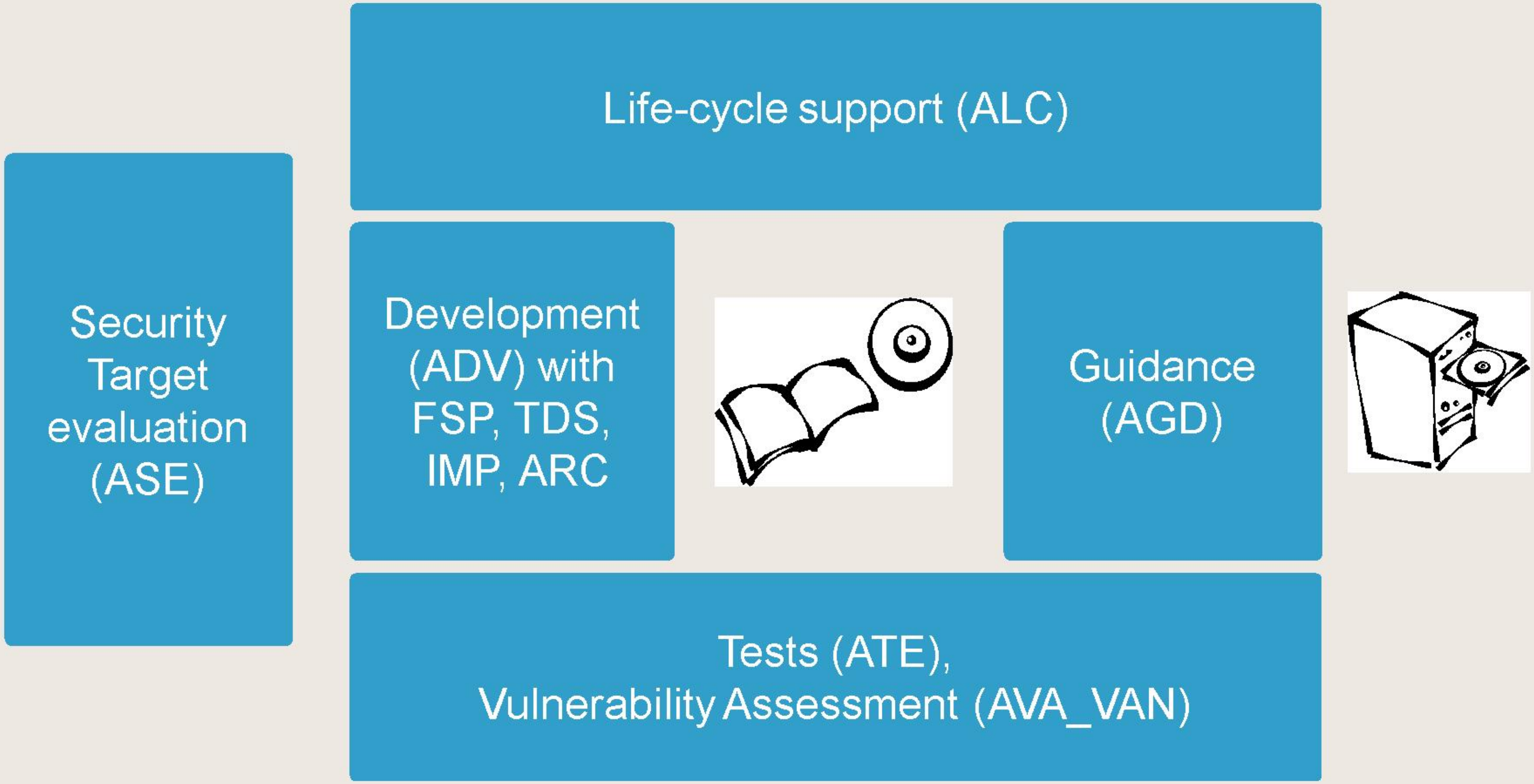
- To perform evaluation tasks efficiently
    - This is what you do
    - And this is where you should stop.
- To perform evaluation correctly
    - Follow above methodology, and
    - This is the terminology you encounter.
- To meet formal accreditation requirements
    - The above, and
    - Remember definitions of:
        - Class/family/element/component
        - AXY_YXZ.x is hierarchical to AXY_YXZ.y iff x>y
        - Conformant/Augmented/Extended
        - …..

Presentation Targets

Describe our final experiences with CCv3.1 Release 1 on a smartcard IC

- □ CC v3.1 evaluation of smart cards
  - ■ ST
  - ■ Security Architecture
- □ Training of CC v3.1 to evaluators
- □ Usefulness of CC

Common Criteria in one slide



Life-cycle support (ALC)

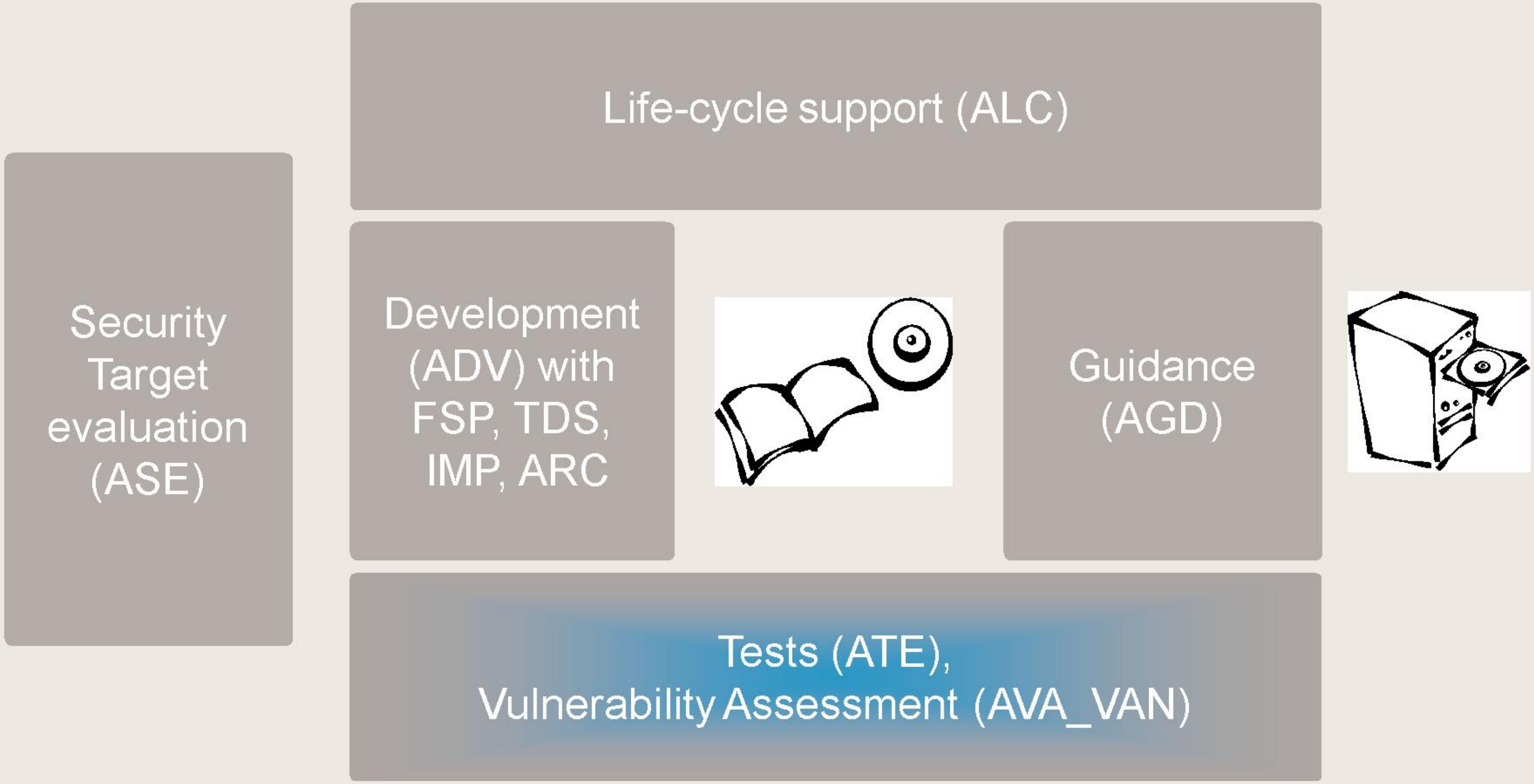
Security Target evaluation (ASE)

Development (ADV) with FSP, TDS, IMP, ARC

Guidance (AGD)

Tests (ATE), Vulnerability Assessment (AVA_VAN)

“Blackbox evaluation” in terms of CC



Life-cycle support (ALC)

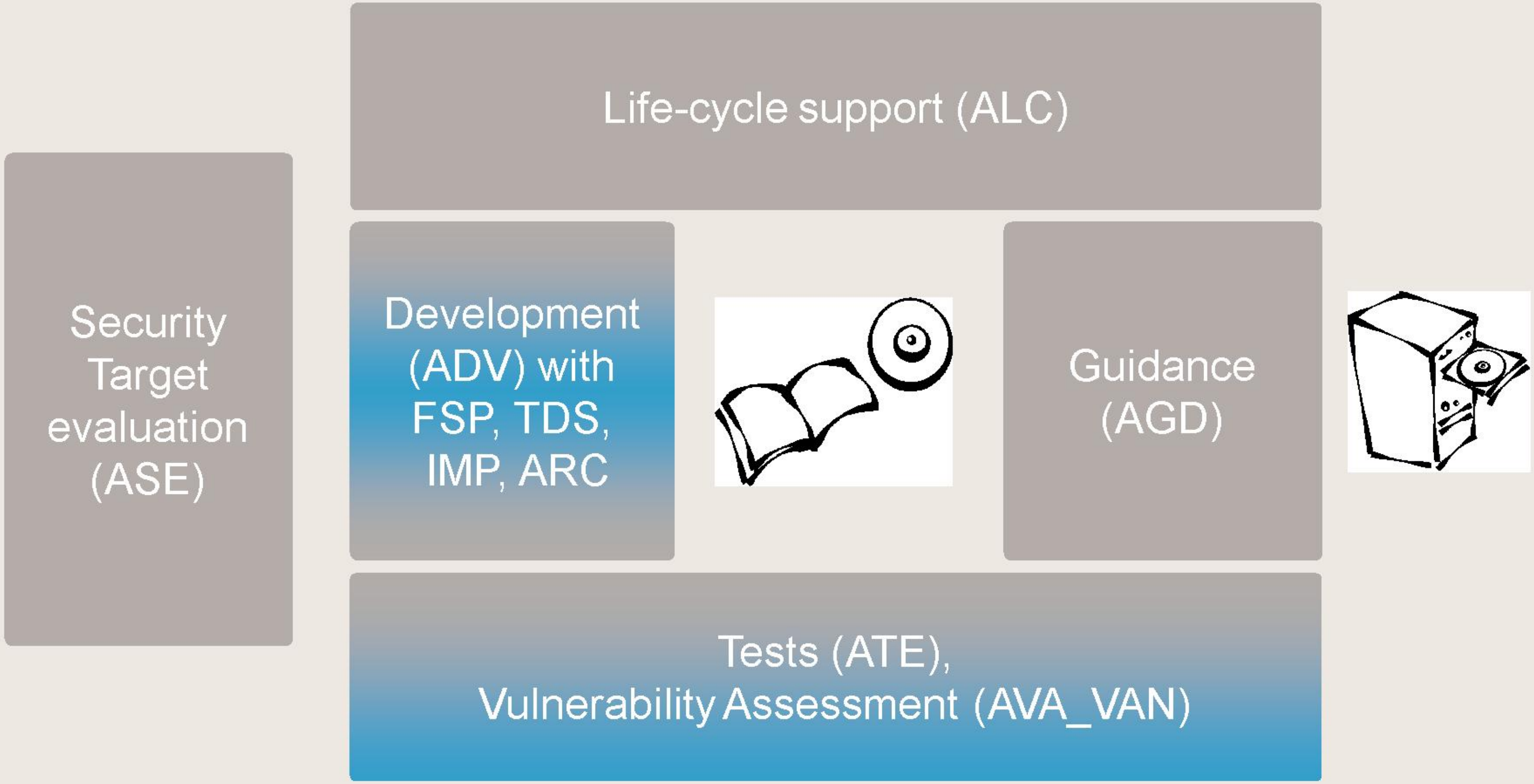
Security Target evaluation (ASE)

Development (ADV) with FSP, TDS, IMP, ARC

Guidance (AGD)

Tests (ATE),
Vulnerability Assessment (AVA_VAN)

Extensive whitebox evaluation in CC terms



Life-cycle support (ALC)

Security Target evaluation (ASE)

Development (ADV) with FSP, TDS, IMP, ARC

Guidance (AGD)

Tests (ATE), Vulnerability Assessment (AVA_VAN)

Extensive whitebox evaluation properties

- Implicit “PP/ST”
  - Fixed functionality
  - Fixed requirements
- “Fixed” methodology
- Design review to focus penetration tests
- Fixed effort approach to penetration testing

Extensive whitebox evaluation properties

- Implicit “PP/ST”
  - Fixed functionality
  - Fixed requirements
- “Fixed” methodology
- Design review to focus penetration tests
- Fixed effort approach to penetration testing

Attack 1, chance 30%
Attack 2, chance 50%
Attack 3, chance 01%
Attack 4, chance 60%

Extensive whitebox evaluation properties

- □ Implicit “PP/ST”
  - ■ Fixed functionality
  - ■ Fixed requirements
- □ “Fixed” methodology
- □ Design review to focus penetration tests
- □ Fixed effort approach to penetration testing

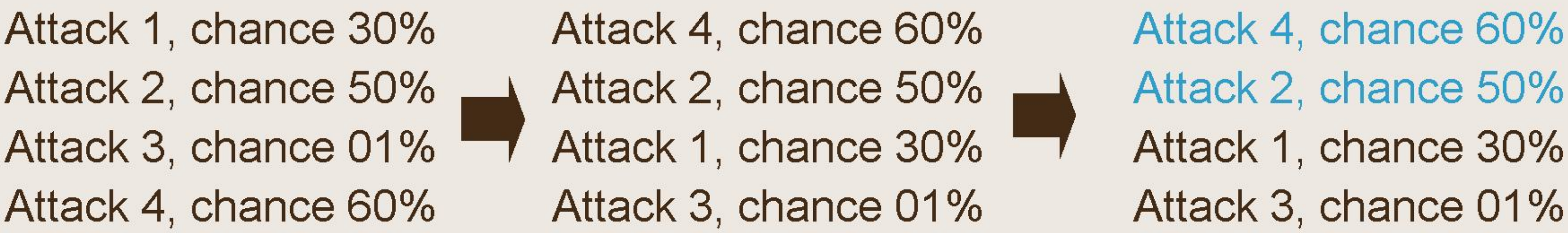
Attack 1, chance 30%
Attack 2, chance 50%
Attack 3, chance 01%
Attack 4, chance 60%

→

Attack 4, chance 60%
Attack 2, chance 50%
Attack 1, chance 30%
Attack 3, chance 01%

Extensive whitebox evaluation properties

- Implicit “PP/ST”
  - Fixed functionality
  - Fixed requirements
- “Fixed” methodology
- Design review to focus penetration tests
- Fixed effort approach to penetration testing



Attack 1, chance 30%
Attack 2, chance 50%
Attack 3, chance 01%
Attack 4, chance 60%

Attack 4, chance 60%
Attack 2, chance 50%
Attack 1, chance 30%
Attack 3, chance 01%

Attack 4, chance 60%
Attack 2, chance 50%
Attack 1, chance 30%
Attack 3, chance 01%

White box versus CC (on one crowded slide)

	White box	Common Criteria
Process	None (very limited versioning)	Versioning, process, site security
Requirements	Not discussed (fixed for process)	Flexible (but mostly fixed)
Design	Review only for attack focusing	Extensive tracing, exclusion of attacks
Functional testing	Not part evaluation, additionally required	Included (typically limited)
Penetration testing	Top x attacks for project budget	Sufficient to exclude all attacks in attack potential
Paperwork “overhead”	Low (high intrinsic alignment with scheme)	Medium CC standard International alignment
Approximate page count	~200 pages	~1500 pages

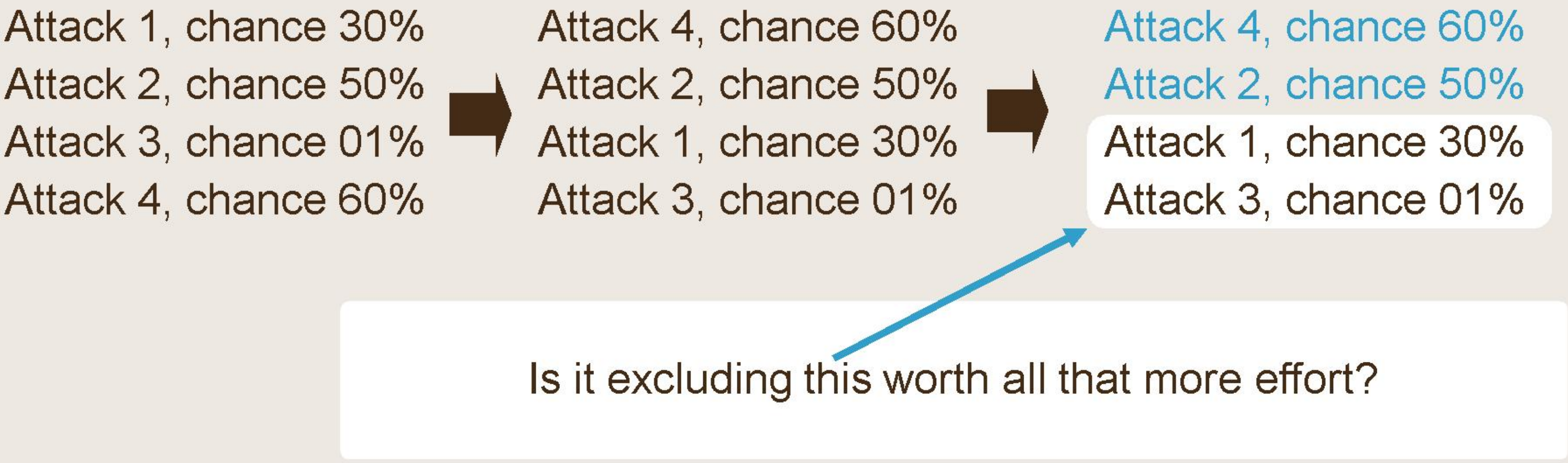
White box versus CC where is the majority of the costs

	White box	Common Criteria
Process	None (very limited versioning)	Versioning, process, site security
Requirements	Not discussed (fixed for process)	Flexible (but mostly fixed)
Design	Review only for attack focusing	Extensive tracing, exclusion of attacks
Functional testing	Not part evaluation, additionally required	Included (typically limited)
Penetration testing	Top x attacks for project budget	Sufficient to exclude all attacks in attack potential
Paperwork "overhead"	Low (high intrinsic alignment with scheme)	Medium CC standard International alignment
Approximate page count	~200 pages	~1500 pages

White box versus CC
where is the added assurance/value (in my humble opinion)

	White box	Common Criteria
Process	None (very limited versioning)	Versioning, process, site security
Requirements	Not discussed (fixed for process)	Flexible (but mostly fixed)
Design	Review only for attack focusing	Extensive tracing, exclusion of attacks
Functional testing	Not part evaluation, additionally required	Included (typically limited)
Penetration testing	Top x attacks for project budget	Sufficient to exclude all attacks in attack potential
Paperwork "overhead"	Low (high intrinsic alignment with scheme)	Medium CC standard International alignment
Approximate page count	~200 pages	~1500 pages

The real questions:
additional assurance by more coverage worthwhile?



Attack 1, chance 30%
Attack 2, chance 50%
Attack 3, chance 01%
Attack 4, chance 60%

Attack 4, chance 60%
Attack 2, chance 50%
Attack 1, chance 30%
Attack 3, chance 01%

Attack 4, chance 60%
Attack 2, chance 50%
Attack 1, chance 30%
Attack 3, chance 01%

Is it excluding this worth all that more effort?

Is the last step worthwhile?

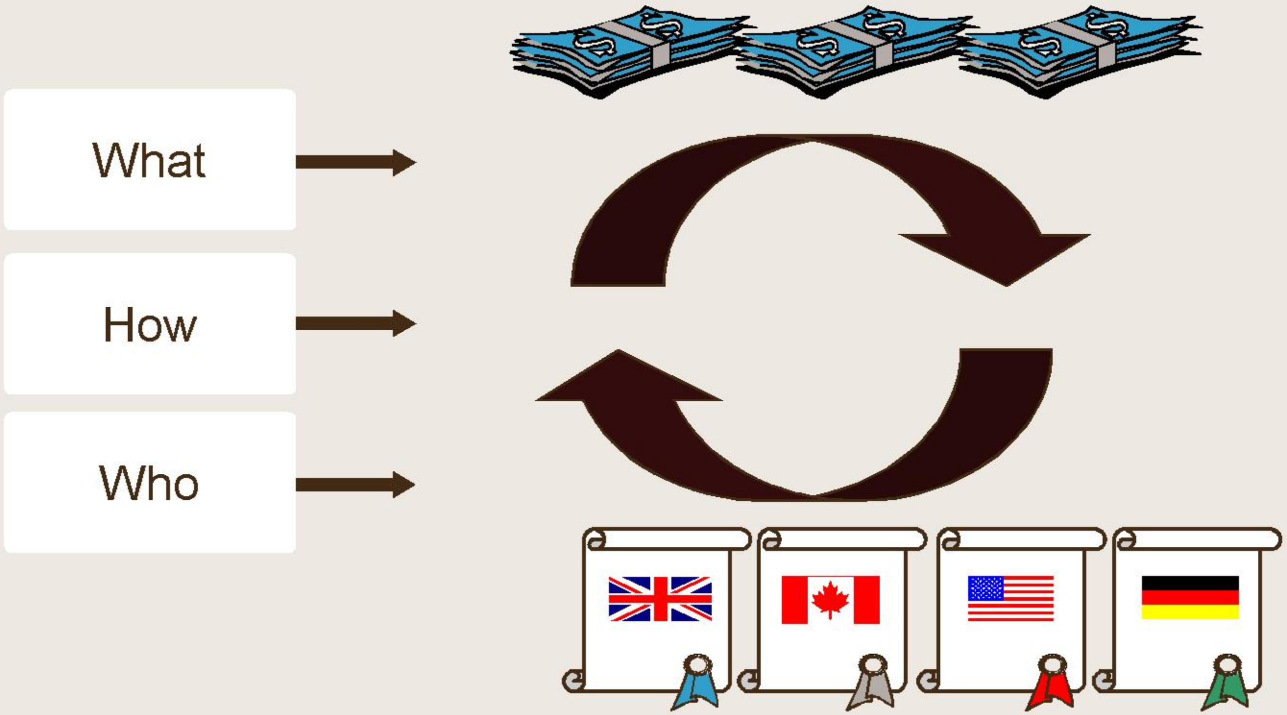
Yes:

- □ ST: holes in security concept
- □ FSP: dubious functionality in not directly SFR-related interfaces (i.e. non-interfering parts)
- □ TDS: construction/interaction allows new attack paths
- □ AGD: guidance misleading or unclear
- □ ALC: TOE and implementation representation are slightly different
- □ ALC_DVS: Site security poor
- □ AVA: reasoning why all attacks are covered has a hole -> points to less likely but not addressed attacks

No:

- > In whitebox evaluations security concept typically is already examined and fixed
- > FSP/AGD: idem
- > TDS/AVA: experienced evaluators will focus on most likely points anyway
- > Remaining missed vulnerabilities are also in field missed

The real questions:
One internationally recognised certificate worthwhile?



Is the one (expensive) CC evaluation cheaper then the (less expensive but more) other evaluations?

Where good labs reduce costs

	White box	Common Criteria
Process	None (very limited versioning)	Versioning, process, site security
Requirements	Not discussed (fixed for process)	Flexible (but mostly fixed)
Design	Review only for attack focusing	Extensive tracing, exclusion of attacks
Functional testing	Not part evaluation, additionally required	Included (typically limited)
Penetration testing	Top x attacks for project budget	Sufficient to exclude all attacks in attack potential
Paperwork “overhead”	Low (high intrinsic alignment with scheme)	Medium CC standard International alignment
Approximate page count	~200 pages	~1500 pages

Presentation Targets

Describe our final experiences with CCv3.1 Release 1 on a smartcard IC

- CC v3.1 evaluation of smart cards
  - ST
  - Security Architecture
- Training of CC v3.1 to evaluators
- Usefulness of CC

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/