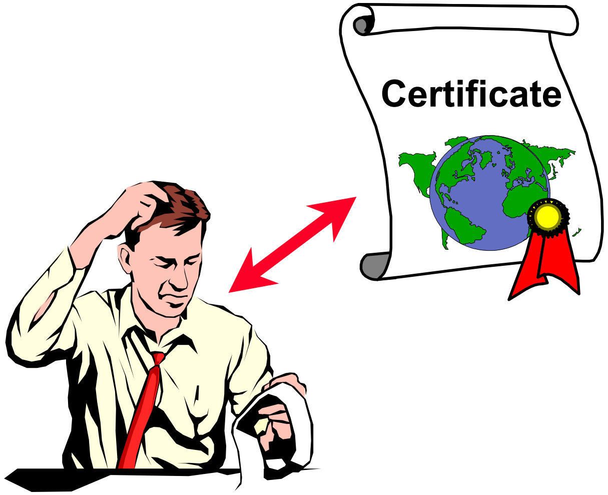
Common Criteria:

How does this Standard work?

Dr. Igor Furgel

T-Systems GEI GmbH
BU ITC Security



T · · Systems ·

What are we speaking about?

- Evaluation Philosophy
- Evaluation and Validation scheme
- Limits of evaluation
- Human factor as the anchor of trust
- Maintenance of evaluation results
- Benefits and restrictions of evaluation

Evaluation philosophy

- In the beginning there were
  - consumer's security needs, and
  - IT products/systems
- How can I gain the confidence in an IT product?
  - I trust in and rely on the developer (by my experience or his reputation) or
  - I explore the product
- But how?
  - Can/shall I do it by myself?
  - Or is it more efficient to outsource this to an expert team due to special know-how and experiences.

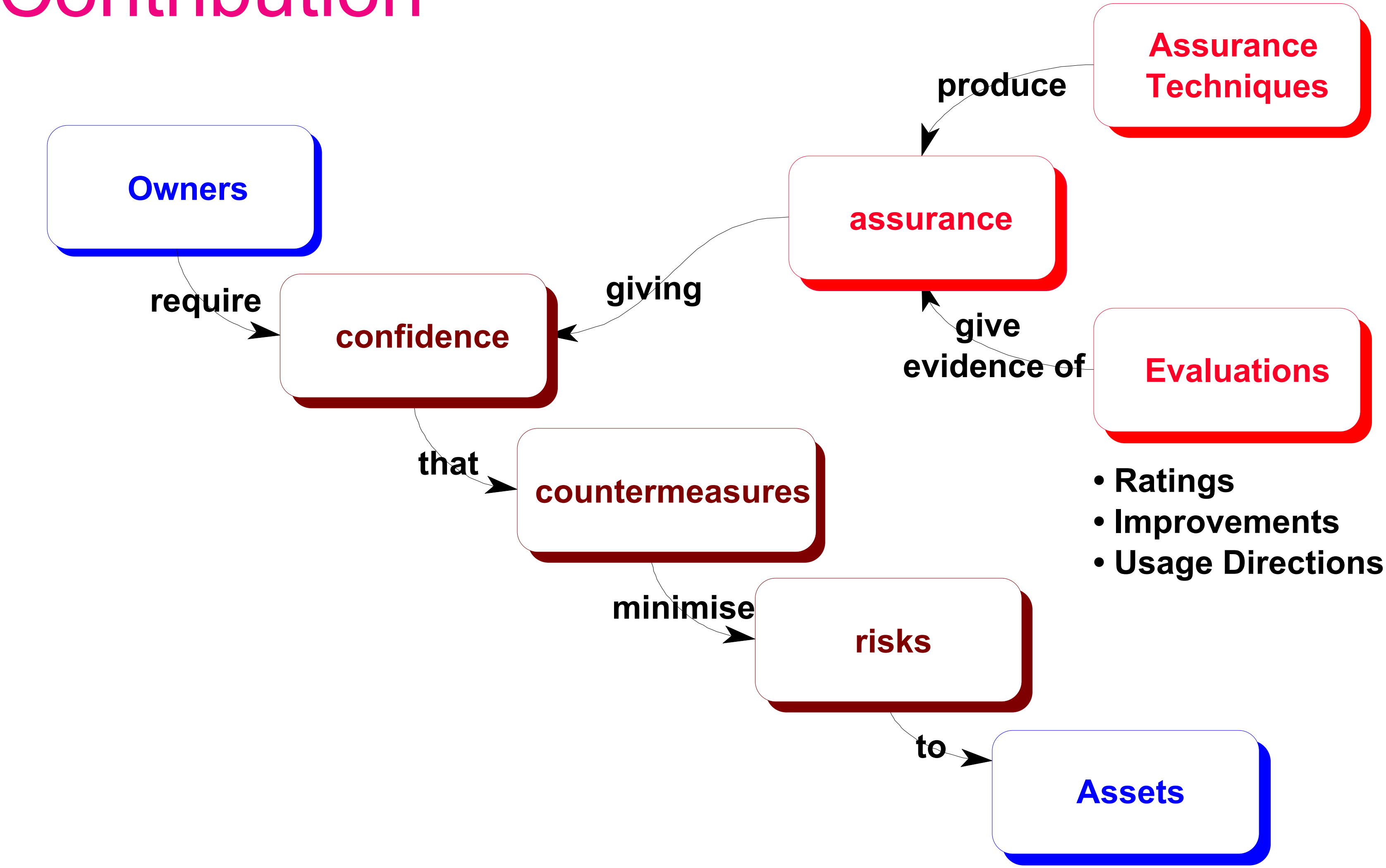
Evaluation philosophy: Assurance, Correctness and Effectiveness

Assurance: the confidence in the security provided by a product.

Correctness: is the idea well implemented?

Effectiveness: is the idea appropriate to cope with the actual security situation?

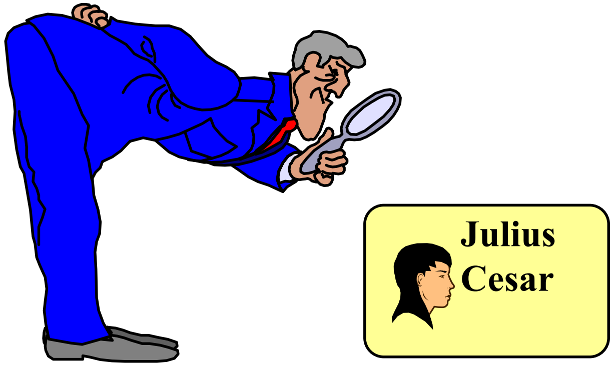
Evaluation and Validation scheme: Contribution



- Ratings
- Improvements
- Usage Directions

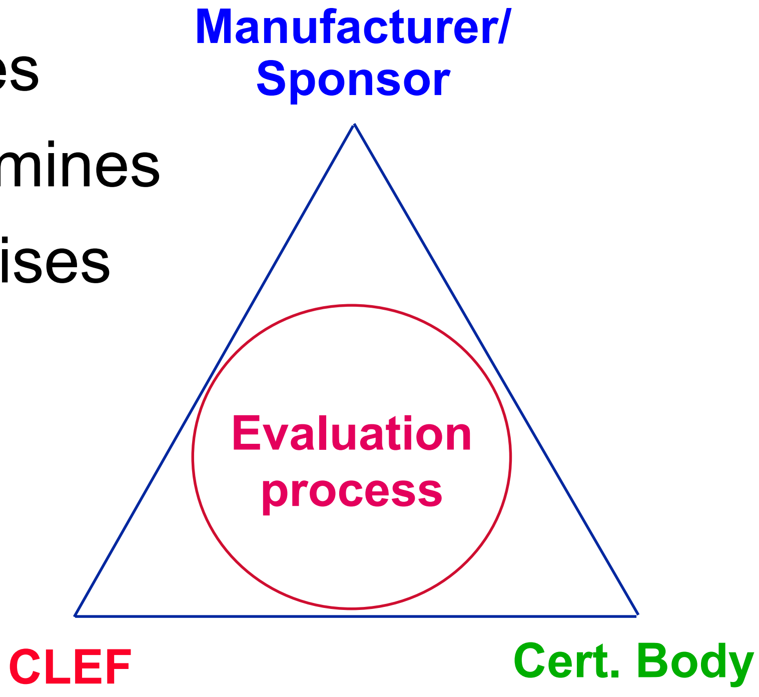
Evaluation and Validation scheme: players

- Human players
- Technical players
- Common metric



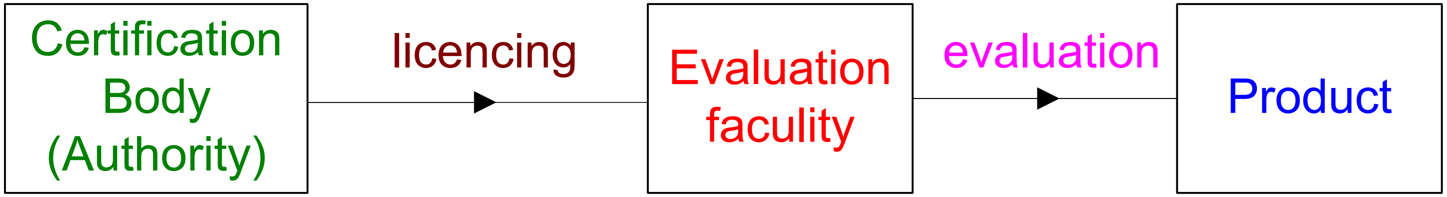
Evaluation and Validation scheme: Human players

- Human players:
  - –manufacturer/sponsor: provides
  - –evaluation facility (CLEF): examines
  - –certification body (CB): supervises



Evaluation and Validation scheme: Human players

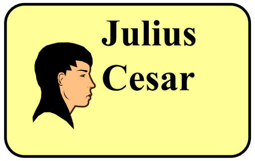
- Certification Body is the anchor of trustworthiness



- Trust transition: If the consumer trusts in the CB, he can also trust in the product certified

Evaluation and Validation scheme: Technical players

- the product

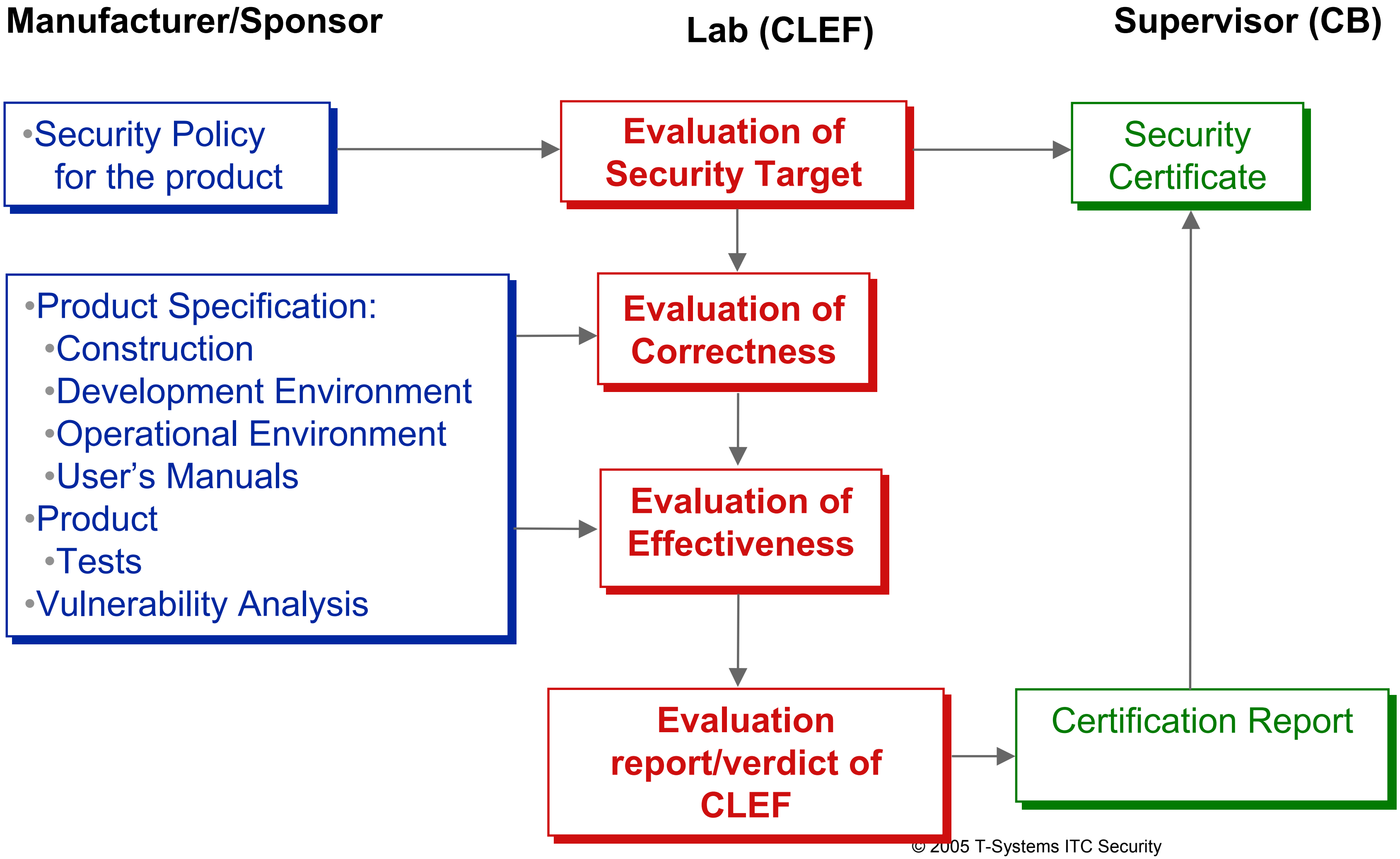


- evaluation tools

Evaluation and Validation scheme: Common Metric

- The common metric of a contemporary evaluation comprises:
  - Criteria
    - Common Criteria (CC)
      - current version 2.2
      - version 3.0 in the comment phase
  - Methodology
    - CEM
  - Interpretations
    - International: CCIMB (CC International Management Board)
    - European: JIL (Joint Interpretation Library)
    - National: Particular national interpretations of the evaluation scheme (e.g. AIS in Germany)

Evaluation and Validation scheme: Succession of evaluation



Manufacturer/Sponsor

Lab (CLEF)

Supervisor (CB)

- Security Policy for the product

- Product Specification:
  - Construction
  - Development Environment
  - Operational Environment
  - User's Manuals
- Product
  - Tests
- Vulnerability Analysis

Evaluation of Security Target

Evaluation of Correctness

Evaluation of Effectiveness

Evaluation report/verdict of CLEF

Security Certificate

Certification Report

Evaluation and Validation scheme: General structure of CC

- Part 1: Introduction and general model (philosophy)
- Part 2: Security functional requirements (catalogue of functional requirements)
- Part 3: Security assurance requirements (catalogue of assurance requirements)
- CEM: Evaluation Methodology

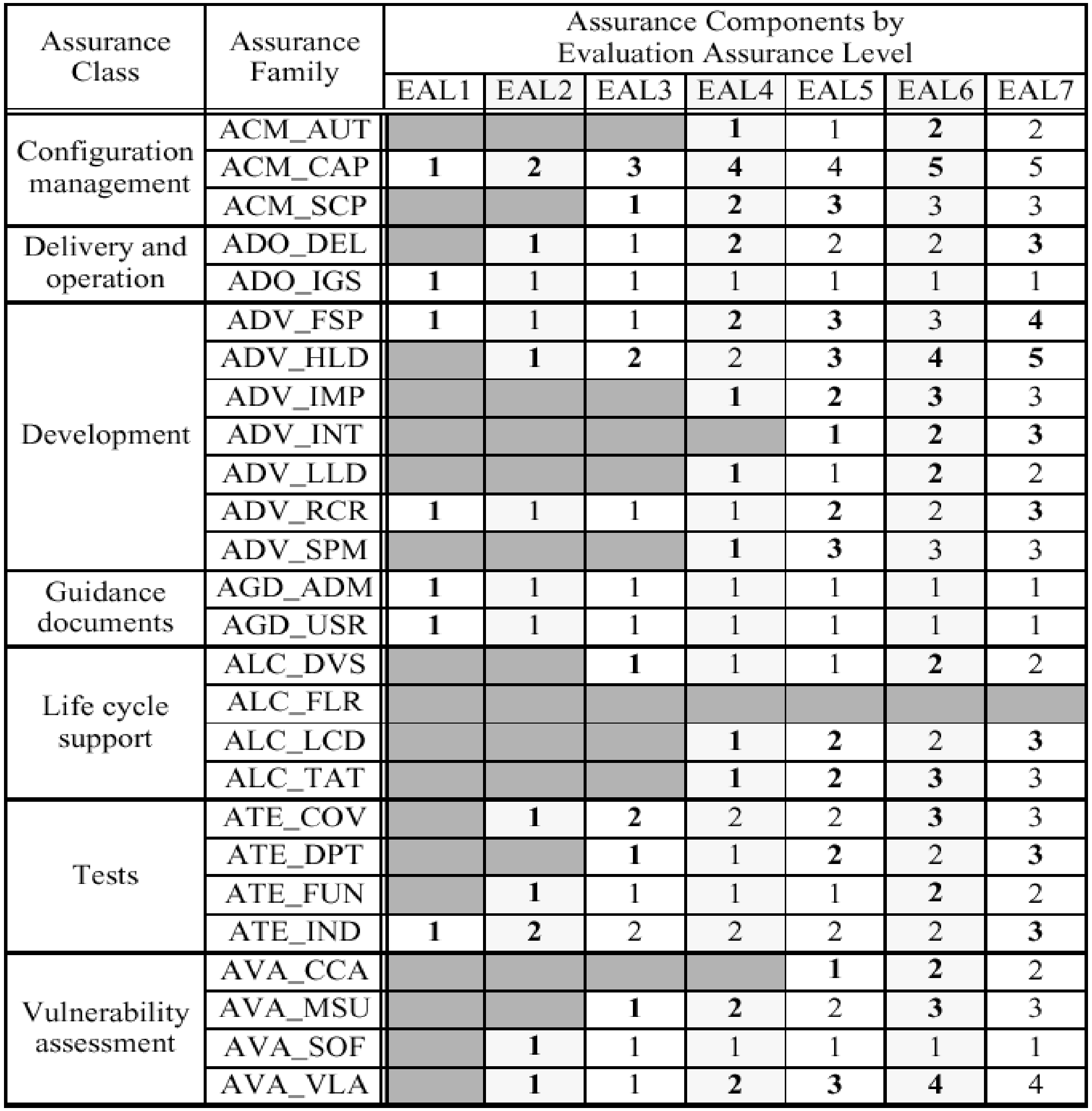
Evaluation and Validation scheme: Evaluation Assurance Levels (EAL)

- Functionally tested (EAL1)
- Structurally tested (EAL2)
- Methodically tested and checked (EAL3)
- Methodically designed, tested and reviewed (EAL4)
- Semi-formally designed and tested (EAL5)
- Semi-formally verified designed and tested (EAL6)
- Formally verified designed and tested (EAL7)

T · · Systems

Evaluation and Validation scheme: EAL Overview for CC2.2

- EAL packages
  - EAL1: pure test, pre-evaluation
  - EAL2: obvious vulnerabilities assessed
  - EAL3: security assessment without specific efforts
  - EAL4: maximum assurance from positive security engineering based on good commercial development practices



Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Delivery and operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Guidance documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Life cycle support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Evaluation and Validation scheme: EAL Overview for CC3.0

- EAL Packages (continue)
  - EAL5: maximum assurance from security engineering based upon rigorous commercial development practices
  - EAL6: high assurance from application of security engineering techniques to a rigorous development environment
  - EAL7: for application in extremely high risk situations and/or the high value of the assets

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	**2**	2	2
	ADV_CMP							
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	**4**
	ADV_SPM					**1**	1	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Security Target evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_CCA					**1**	**2**	2
	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

© 2005 T-Systems ITC Security
Dr. Igor Furgel: Common Criteria: How does this Standard work?
Security & Trust for the deployment of information & telecommunication systems
29th of March, 2005, page 15.

Scheme: Transition CC2.2 -> CC3.0

Assurance class	Assurance Family CC2.2	Assurance Family CC3.0
Configuration Management	ACM_AUT	--
	ACM_CAP	-- (ALC_CMC)
	ACM_SCP	-- (ALC_CMS)
Delivery and operation	ADO_DEL	-- (ALC_DEL)
	ADO_IGS	-- (part of ADV_ARC)
Development	ADV_LLD (+ ADO_IGS)	ADV_ARC
	--	ADV_CMP
	ADV_FSP	ADV_FSP
	ADV_IMP	ADV_IMP
	ADV_INT	ADV_INT
	ADV_SPM	ADV_SPM
	ADV_HLD	ADV_TDS

Scheme: Transition CC2.2 -> CC3.0

Guidance documents	AGD_USR	AGD_OPE
	AGD_ADM	AGD_PRE
Life-cycle support	-- (ACM_CAP)	ALC_CMC
	-- (ACM_SCP)	ALC_CMS
	-- (ADO_DEL)	ALC_DEL
	ALC_DVS	ALC_DVS
	ALC_FLR	ALC_FLR
	ALC_LCD	ALC_LCD
	ALC_TAT	ALC_TAT
Security Target evaluation	ASE	ASE
Tests	ATE_COV	ATE_COV
	ATE_DPT	ATE_DPT
	ATE_FUN	ATE_FUN
	ATE_IND	ATE_IND
Vulnerability assessment	AVA_CCA	AVA_CCA
	AVA_VLA	AVA_VAN
	AVA_SOF	-- (AVA_VAN)
	AVA_MSU	-- (AVA_VAN)

Evaluation and Validation scheme: General benefits of an independent evaluation

- Impartiality
- Repeatability
- Reproducibility
- Comparability

- -> it means **more objectivity**, although evaluator's judgement and background knowledge are of a subjective nature.

Succession of evaluation: Back to the consumer/operator

- Now there are the product and the security certificate. What does the consumer (often the operator of the product/system) have to do else?

  - He has to decide, whether the security features of the product match his security needs.

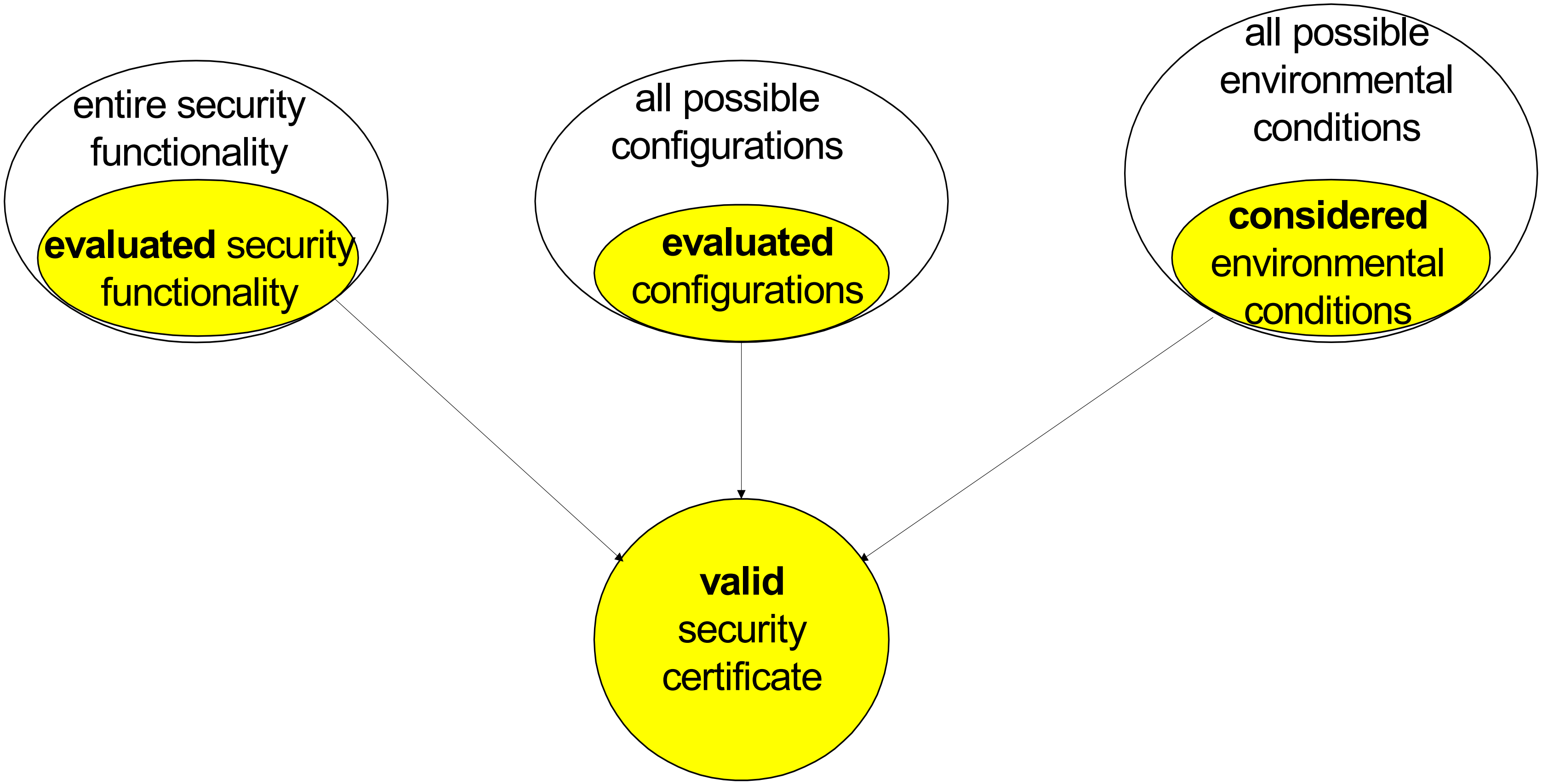
- How can he do it?

Limits of evaluation: Scope

- The scope of a concrete evaluation is exactly defined in the Security Target.

- The Security Target declares:
  - the sub-set of the security functionality being under evaluation
  - the sub-set of the different configurations of the product having to be evaluated
  - the environmental conditions (technical and organisational) being assumed and having to be fulfilled

Limits of evaluation: Certificate validity


entire security functionality
evaluated security functionality
all possible configurations
evaluated configurations
all possible environmental conditions
considered environmental conditions
valid security certificate

Limits of evaluation: Certificate validity

- **Very important for consumer/operator: A security certificate is valid only for the scope of evaluation defined in the Security Target.**
  - The consumer shall compare the information delivered by the ST with his security needs and merely after having done it decide on using the product.
  - He shall operate the product/system only under conditions having been in the scope of evaluation. Else he operates the product **out of validity of the security certificate**. The question of liability should not be underestimated in this case.

Human factor as the anchor of trust

- An IT product/system
  - offers different configuration options
  - shall be maintained, etc.

- We cannot gain assurance based only upon the technical measures: The organisational – **personal and procedural** – measures are important as well.

Human factor as the anchor of trust: Organisational measures: Operator

- The operator of a certified IT product/system shall run it under conditions having been in the scope of evaluation: **He shall also enforce each organisational measure!**

- **The question of plausibility of the assumptions defined in the Security Target for a product/system can primarily be answered by the consumer/operator: He shall know, whether he can implement and enforce the organisational measures assumed.**

Maintenance of evaluation results

- Suppositionally, a product has already gained the security certificate. But time never stops: New attack techniques can be invented, so that the assessment of effectiveness shall be reconsidered.

- Consumer/operator: how can I keep the validity of a security certificate in a changing world?

- The re-certification/re-evaluation or/and maintenance procedures can be applied to the product for keeping the security certificate up-to-date.

Benefits and restrictions of evaluation

- **Benefits**:
  - –clear alignment with the actual security needs
  - –improve security
  - –improve quality (clear concept; control, supervision)
  - –eliminate flaws (independent opinion)
  - –product documentation (keep Know-How)

  - –**more confidence** in security capability of an IT product for its operator.
  - –**more objectivity** because of independent evaluation and certification

Benefits and restrictions of evaluation

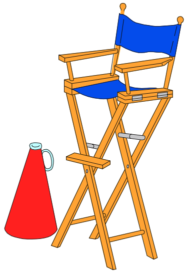
- **Restrictions**:
  - –Consumers will still need to review the information given by evaluation results carefully and assess its applicability to his special needs.
  - –Consumer shall enforce the assumptions about the method of use of the product and its operating environment as well as other conditions confining the validity of the assurance assessment.

Dr. Igor Furgel

T-Systems ITC Security

Rabinstrasse 8
53111 Bonn

☎ +49 (228) 9841-512
🖹 +49 (228) 9841-60
💻 igor.furgel@t-systems.com



T · · Systems ·