World Class Standards

SECURITY EVLUATION&TESTING: SET FRAMEWORK

Contribution to

ETSI MTS#53 Meeting

ETSI Sophia Antipolis, January 18-19, 2012:

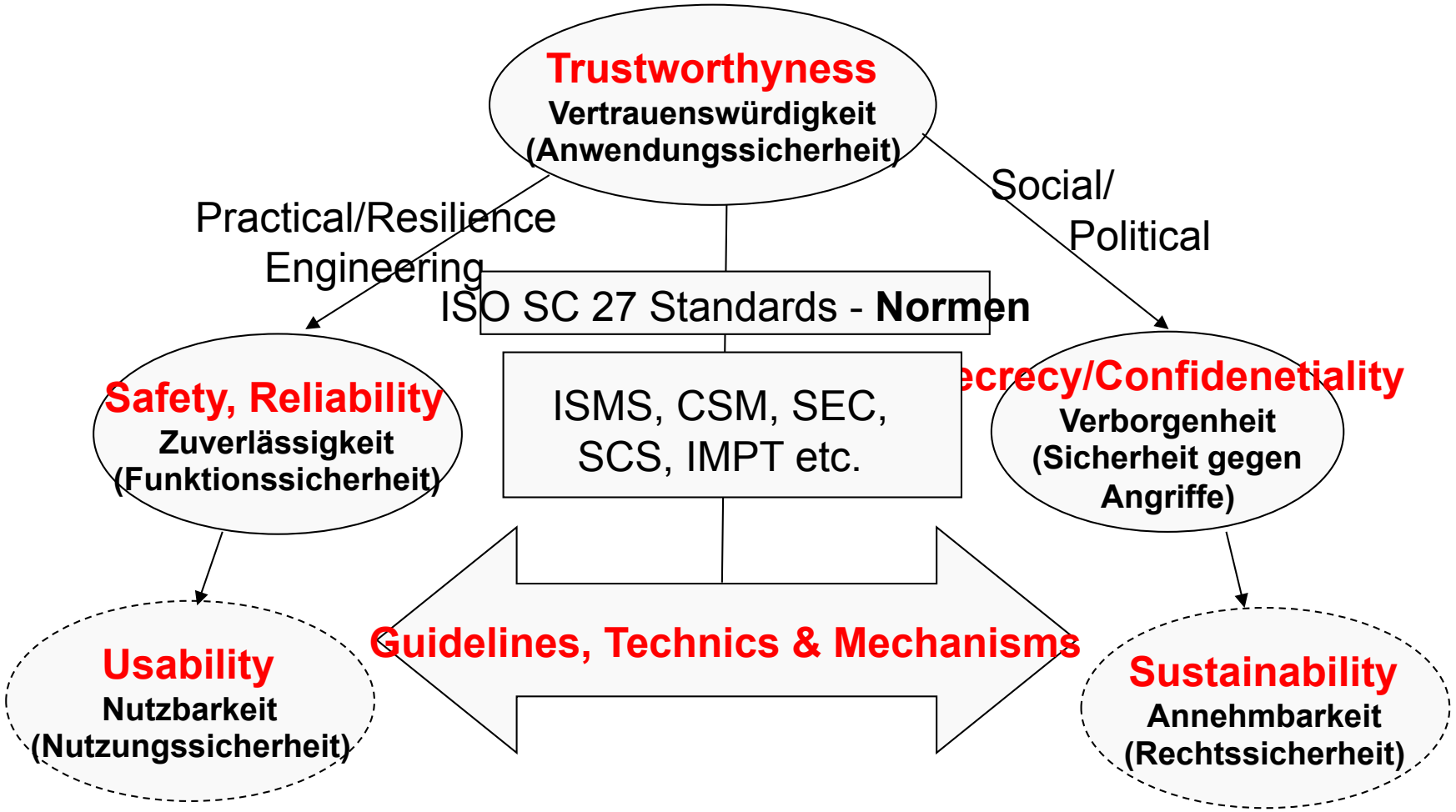
Jan deMeer, ssl.eu GmbH Berlin,

Siv Hilde Houmb, Scott Cadzow

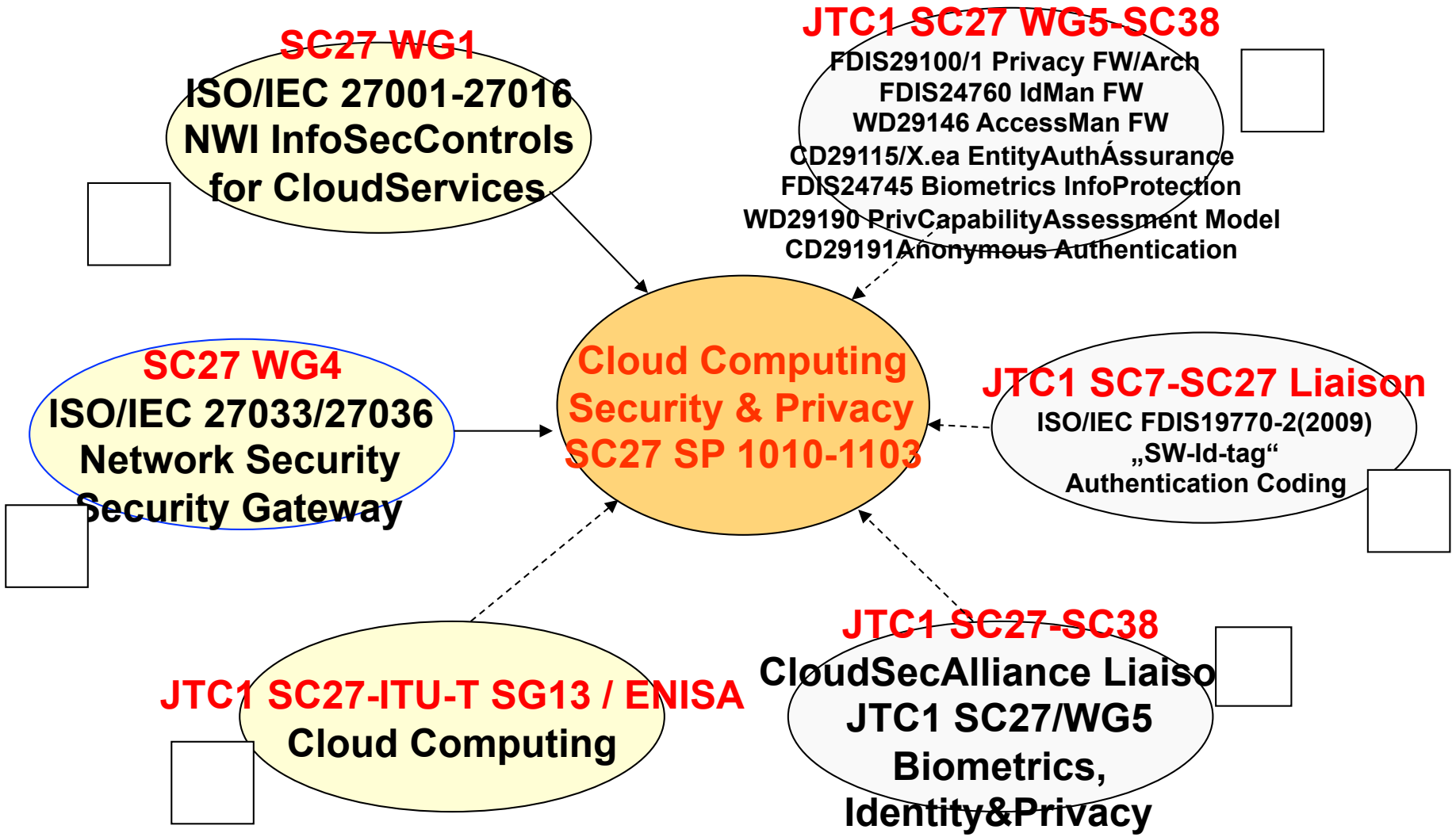
SET FW Sources - Resilient Networks GN and Services

- ***Directive 2009/140/EC of European Parliament and Council,* chapter IIIa, 'Security and integrity of networks and services', article 13a**
  - '… undertakings providing public communications networks or publicly available electronic communications services … [observing] a breach of security or loss of integrity that has had a significant impact on the operation of networks or services' [have to be notified to National Regulatory Authorities]
  - **ENISA Measurement Frameworks and Metrics**
    - Information Security Metrics
      - Incident – Vulnerability – Patch – Application - Configuration
  - **ISO27001/2/4:2009 ISMS**
    - Security Requirements & Security Control Objectives

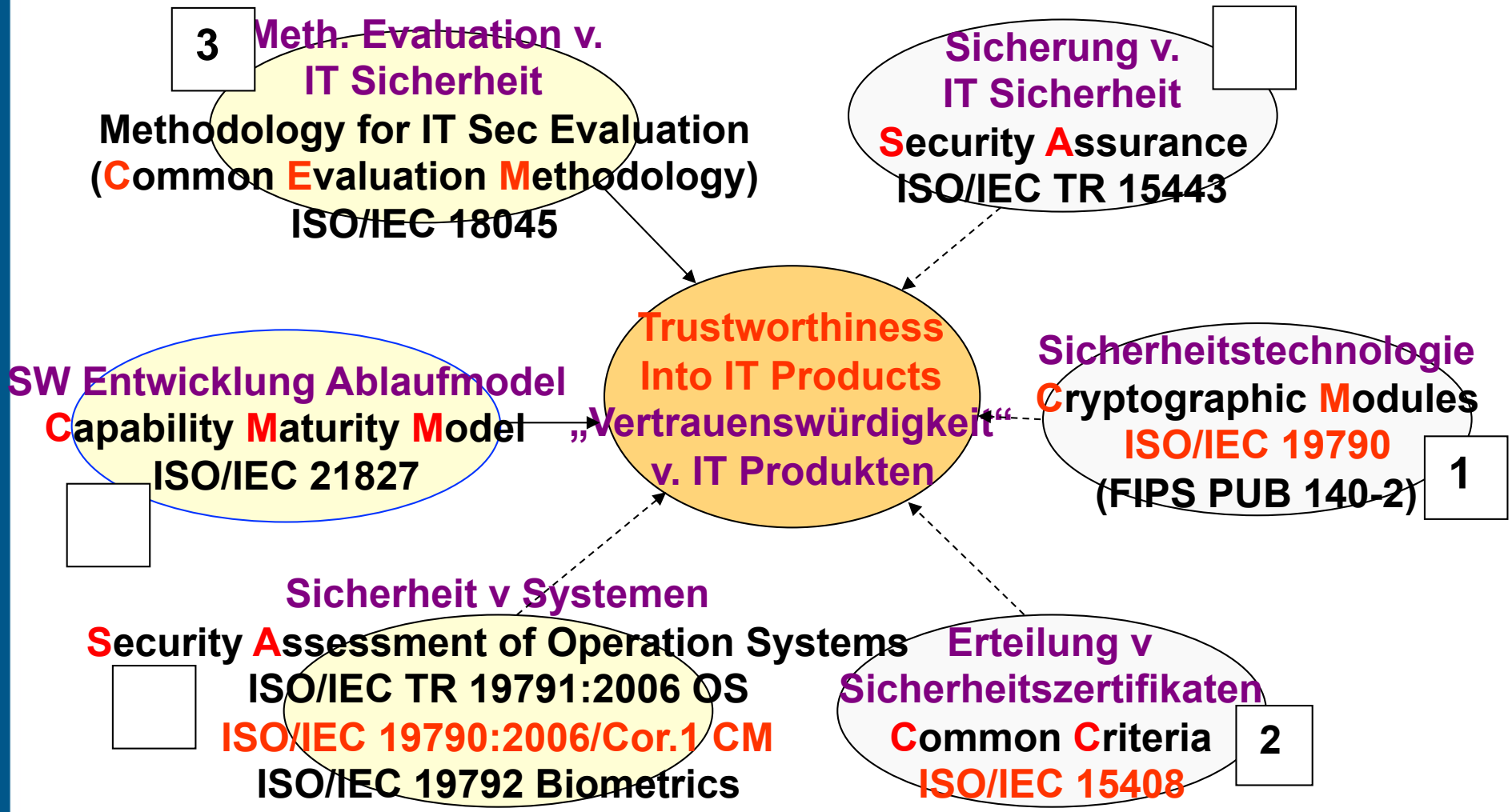
SET FW Sources - ISO Safety & Security Schemes
DIN NIA 27/ ISO SC27 IT Security Approach



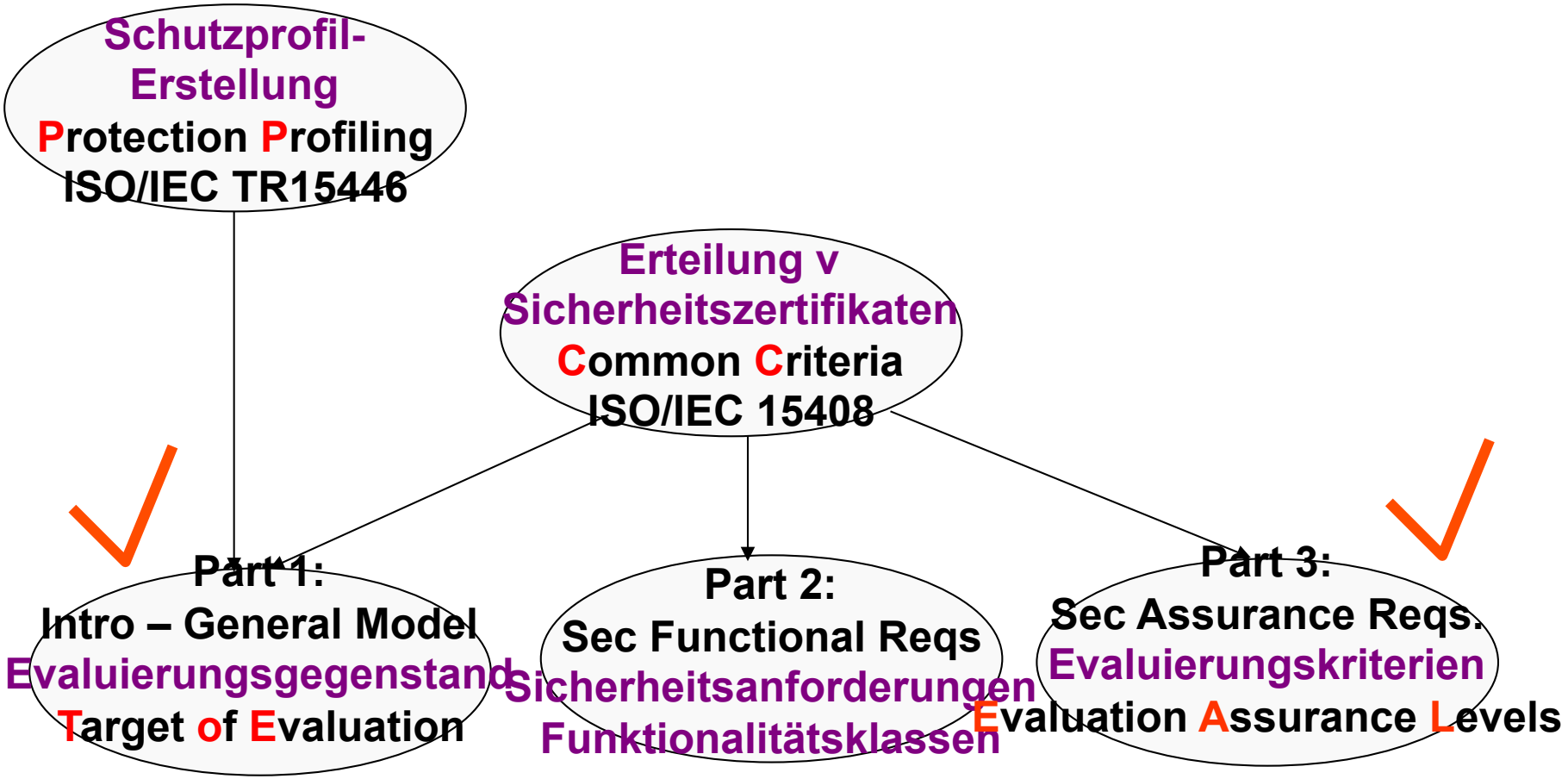
SET FW Sources - ISO Safety & Security Schemes: SC27 N10027/28/29 Study Period Report (NWI)



ST FW Sources -ISO Safety & Security Schemes: Security Evaluation Criteria (ISO WG3)



SET FW Sources - ISO Safety & Security Schemes: ISO/IEC 15408 Common Criteria Overview



Jan deMeer,

SET FW Sources - NGN Security & Resilience Architecture

- **ETSI TISPAN 07 TS 187 001 – NGN Security Infrastructure**
  - stakeholder model with 7 actors
  - 5 Use Cases with respect to Resilience
  - NGN Subsystems
- **ETS TISPAN 07 003 – Security Architecture**
  - NGN Security Services
  - NGN Security Domains
  - NGN Security Policies

SET FW Sources - Safeguarding Principles

- Safeguarding according to ISO/IEC 27001/2/4
  - to counteract security risks, i.e. By inventing Security Control Techniques
  - -> PDC Resilience Controls
    - **P**reventive Controls before threats become possible
      - e.g. to exclude users from servicing that are not authorized
    - **D**etective Controls during a threat that happens
      - e.g. to detect the reasons of threatening in real time
    - **C**orrective Controls after a threat has happened
      - e.g. to minimize loss and destruction and to reset system to safe and secure operation state

SET FW - Security Functional Classes (acc. to TISPAN07 TS187 001)

- **Security of Users**
  - Identification and Authentication
  - Access Control
  - Data Privacy
  - Protection of Personal Identifying Information (PII)
- **Security of NGN Infrastructure**
  - System Intergrity
  - System Resilience
- **Security of NGN Communication**
  - Integrity of Transferred Data
  - Confidentiality of Transferred Data
- **Key Management**
- **Assurance**

SET FW – Stakeholder Model (acc.to ETSI TISPAN 07 TS 187 001)

NGN Stakeholders (= UML Actors)

Security Objectives depend from Actor Roles

Stakeholder Specification

[ActorName: NGNRoles, (ListOfHasRelationships)]:

[**E**nd**U**ser: Srvc-Receiver(push)/Srvc-Initiator(pull), (CP,SP,RA,MF)]
[**C**ontent**O**wner: Content-ProviderForDistribution, (CP,RA)]

[**C**ontent**P**rovider: Content-Distributor-OnD/BrCst/MuCst, (CO,EU,SP)]
[**R**egulatory**A**uthoritory: Privacy/DtPro/SafetyProvider, (SP, EU, CP)]

[**L**awEnforcement**A**uthority: **L**awful**I**nterception / **D**ata**R**etention - DataRecipient, (SP)]

[**M**anu**F**acturer: SW/HW-Provider, (RA,SP,EU)]

[**T**rusted**T**hird**P**arty: PKI-Services, (SP, EU, CP)]

SET FW – Authentication Actor Model acc. to ETSI TS 187 003 v3.4.3 (1)

- Generic Model for Challenge-Response Authentication:

- **Key Manager** to manage and distribute keys to active agents
  - **C**ertification **A**uthority in **P**ublic **K**ey **I**nfrastructure using X.509 Certificates

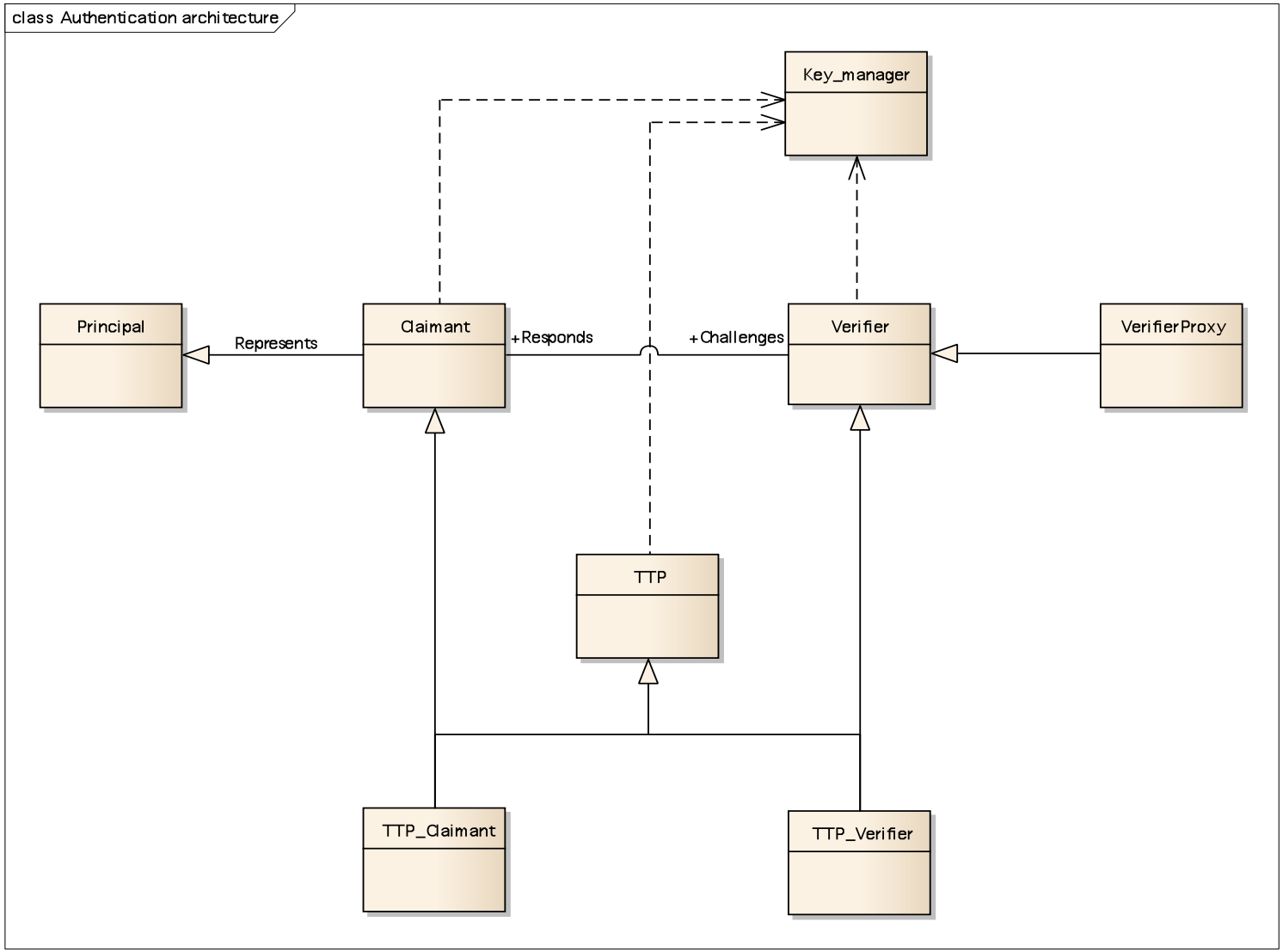
- **Verifier** to initiate and be in charge of Authentication Process
  - Authentication Proxy may carry out verifier‘s role

- **Principal** is an entity whose identity can be authenticated

- **Claimant** to represent principal for purpose of authentication, i.e. entity being authenticated
  - Responsibel to supply correct response to challenge

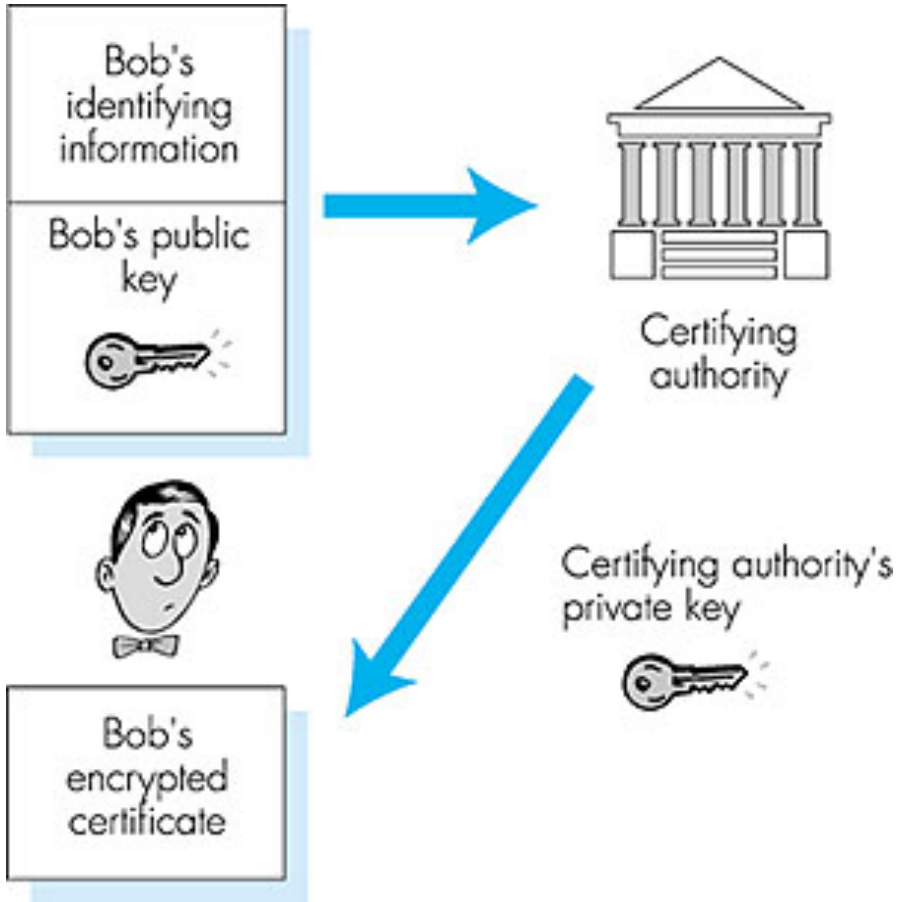
- **T**rusted **T**hird **P**arty to act as special case of proxy either of verifier or claimant

SET FW – Authentication Actor Model acc. to ETSI TS 187 003 v3.4.3 (2)

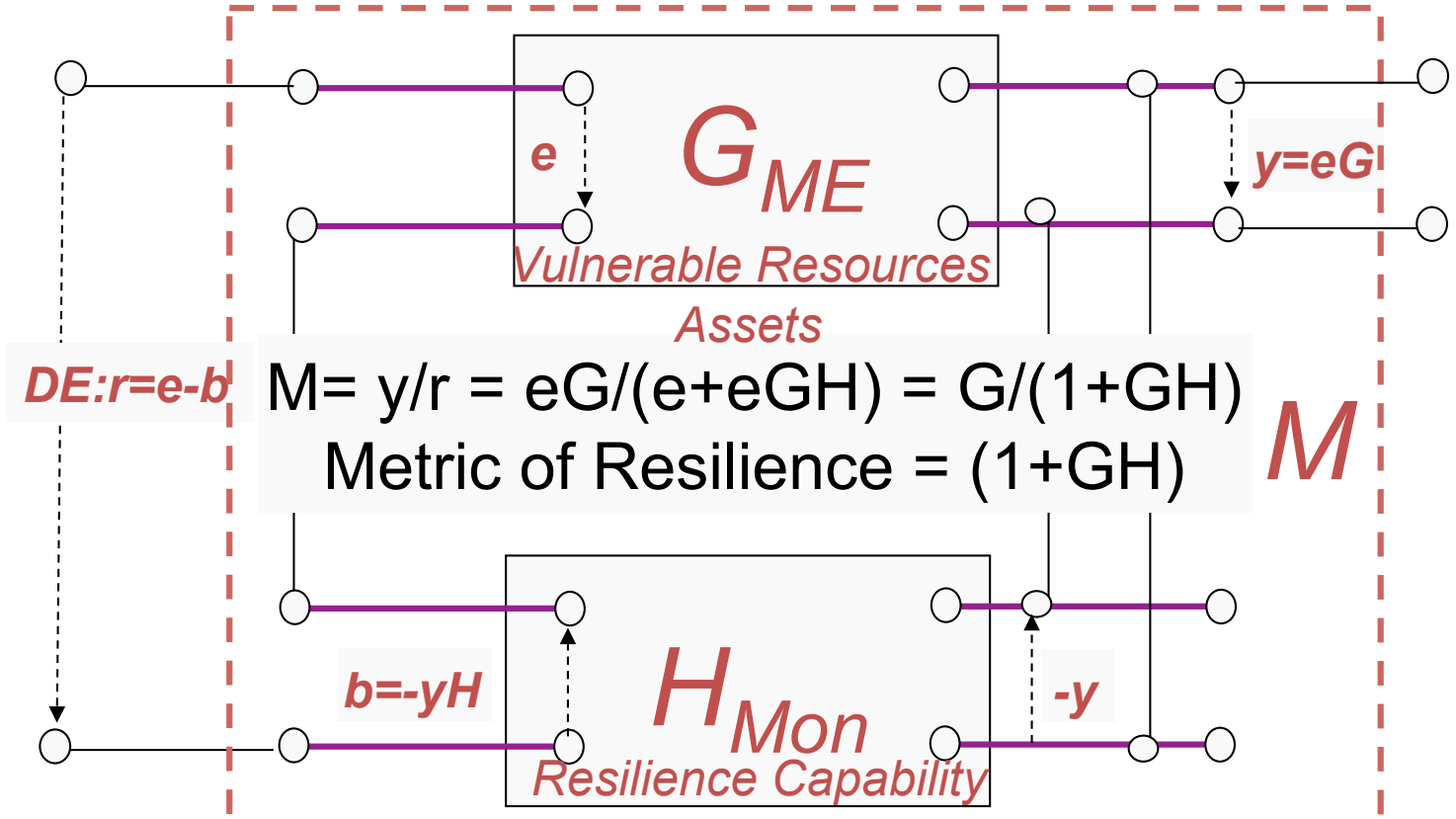


SET FW – Authentication Actor Model acc. to ETSI TS 187 003 v3.4.3 (3)

- Challenge-Response Authentication (Security Algebra):
  - **C**ertification Authoritxy == Key Manager
  - **B**ob == Principal
  - **A**lice == Verifier, Claimant
  - Principal: $[Id, e]_B$
  - register: $IdInfo_B\ PuK_B$ -> $IdProof_B$
  - KeyMgr: $[d_C(IdProof_B)]_C$
  - Certify: $IdProof_B\ PrK_C$ -> $Cert_B$
  - Verifier:$[e_C(Cert_B)]_A$
  - Challenge: $Cert_B\ PuK_C$ -> $IdProof_B$
  - Claimant: $[IdProofB]_A$
  - Response: $IdProof_B$ -> $PuK_B\ IdInfo$



Integrated Assets - Actors Model – Metric of Security Resilience



- **G,H** are assets/resource-consuming Actors:
  - **ME**: Managed Entity + **DE**: Decision-making Element
- **y** is targeted system state
- Embedded System Behahior is gradient **GH, i.e.** positiv or negativ,
- Gradient **GH >1** strengthens, **GH <1**, weakens, **GH <0** out-of-control !

SET FW - Integrated Assets–Actors Model NGN Resilience Dependencies(1)

Resilience means, System shall be capable, to operate compliant to the **reference signals r** !

A system turns vulnerable iff the **targeted system state y** gets out of control,

i.e. the **gradient** comprising vulnerability * resilience is G*H=-1

In other words **y** is unknown for fixed reference signals **r**

Danger: A safe System y=eG could become vulnerable (risky) by inventing a Resilience Component **H** that influences System Gradient in a destructive way, i.e. gradient gets negative!

SET FW - Integrated Assets-Actors Model NGN Resilience Conclusions

Basically in order to eliminate **Effects of failures** Issued by

diverging results wrongly computed from control commands u->y

Diverging inputs wrongly derived from reference commands r

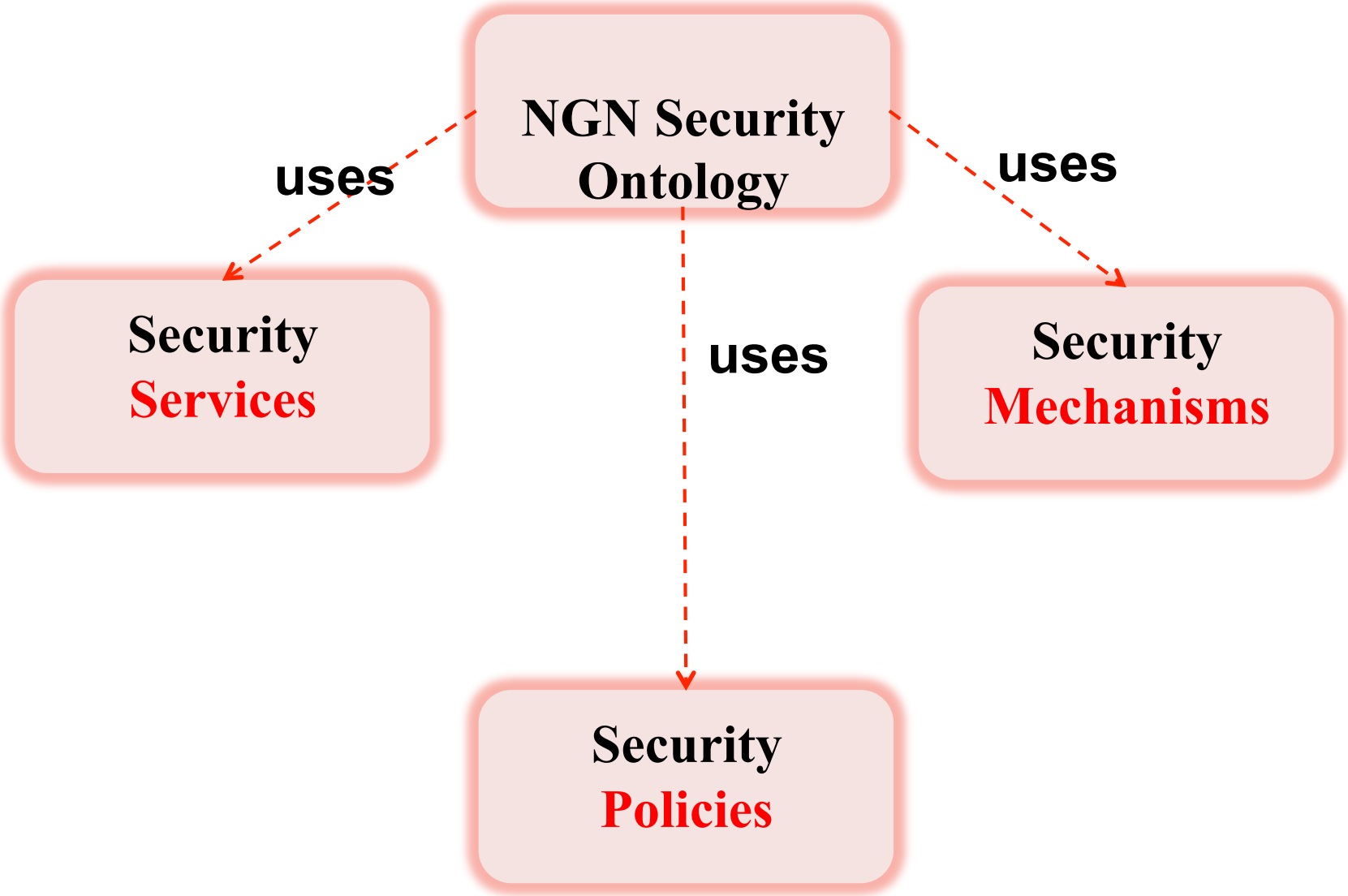
To achieve **System Stability** by providing Activity Control

To achieve **System Reliability** by providing Asset/Resource Control

To achieve **System Robustness/Resilience** by providing Interference/ Jamming Control

To achieve **System Safety/Availability** by providing Sensitivity Control to internal function performances

SET FW - ETSI TISPAN07/MTS – NGN Security Guidelines



SET FW - ETSI TISPAN07/MTS – NGN TVR-Analysis Guidelines (1)

A Security Environment

a.1 Assumptions on the ToE

a.2 Assumptions on the ToE environment

a.3 Assets

a.4 Threat agents

a.5 Threats

a.6 Security policies (OPTIONAL)

B Security Objectives

b.1 Security objectives for the ToE

b.2 Security objectives for the ToE environment

C IT Security Requirements

c.1 asset security requirements

c.1.1 asset security functional requirements (ISO 15408)

c.1.2 asset security assurance requirements

c.2 Environment security requirements (OPTIONAL)

D Application notes (OPTIONAL)

E Rationale, that refers to the goal and purpose of TVRA as defined in TVRA step 1 and recorded in the eTVRA ToE Description table.

Security Evaluation&Testing FrameWork: General Requirements

- General Evaluation Requirements:
  - Support Design for Assurance
  - Support Privacy by Design
  - Support Security by Design

  - Evaluate Performance , QoS
  - Evaluate Security Properties CIAAA
  - Evaluate Privacy

  - Balance Trade-off:
    - QoS vs. Security Privacy
  - Cost trade-off

Security Evaluation&Testing Framework: Goal Definition

- Security Evaluation Goal Definition:
  - Countermeasures must be evaluated to be sufficiently and correctly implemented
  - Evaluation is an effort to measure degree of which countermeasure requirements are implemented by ST, PP, ToE!
  - Sufficiency is defined in terms of EAL1 to EAL7
  - Correctness means that a certain countermeasure does semantically exact „close the door“ to a certain threat or vulnerability
  - Measurement is done by means of tool platform used to get heuristic/tested measures of providing confidence to compliance between requirements (model) and implementation (system).

Security Evaluation&Testing Framework: Task Definitions

1. identify the components of the Security Evaluation System-Model for NGN-based Systems/Applications: (Security Architecture, Smart Metering), i.e. ToE Environment (TR1870002v3.0.5, fig.G.2, pp105)

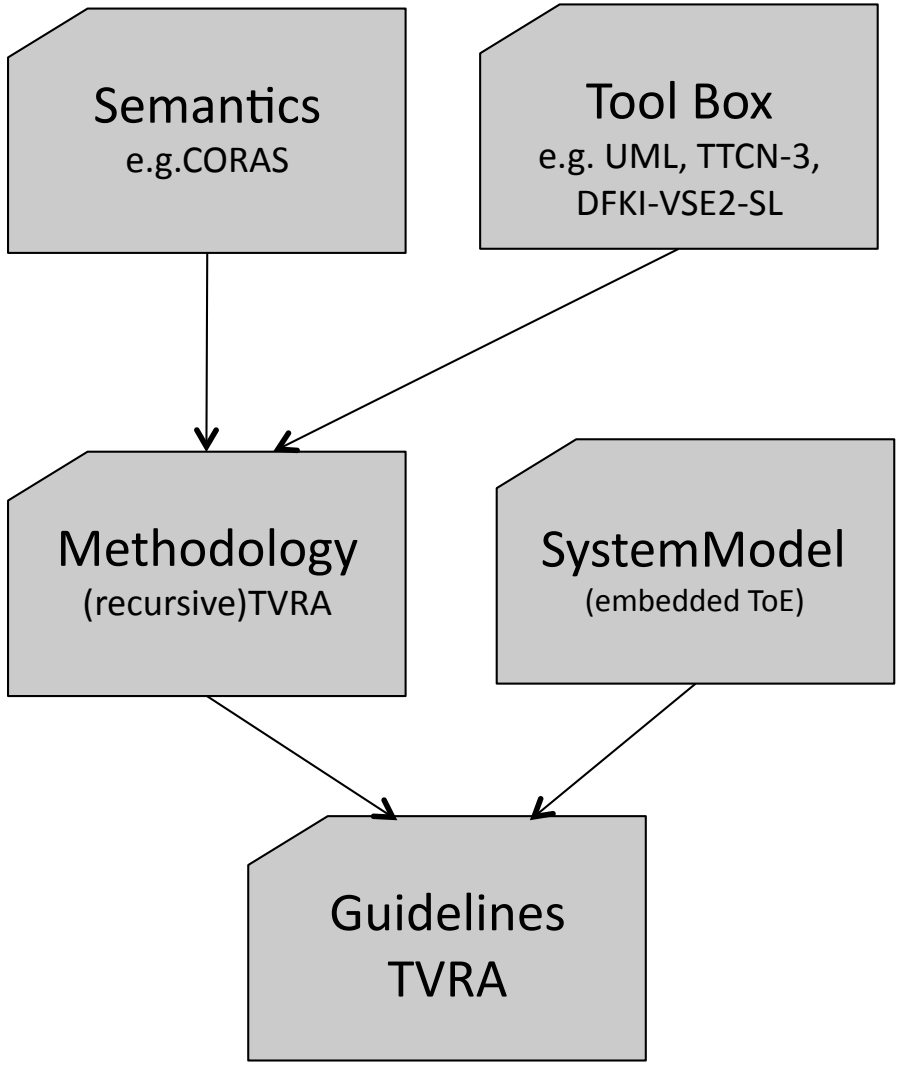
2. identify a Security Evaluation Methodology in terms of Security-related components, i.e. iST, PP, ToE: (TVRA Risk Metrics, TVRA Methodology, stencil for ToE, Authorization Model)

3. identify an appropriate Security Evaluation Semantics, e.g. CORAS, to make decisions on measurements

4. identify a Security Evaluation Tool Box (Platform), e.g. MTS-TTCN-3, TVRA, UML, Security Logics, DFKI-VSE/SL etc. compliant with the Security Evaluation Semantics (TVRA Updating)

5. identify Security Evaluation Guidelines on how to achieve Sufficiency or Correctness with respect to the Semantics and by means of tool-box application (Remote Access Use Case)

SET FW - Methodological Dependencies



SET FW - ETSI TVRA Methodology

1. **TVRA I**nformation **M**odel to gain Security-related System Dependencies

2. **TVRA D**ata **B**ase to retrieve security-related system data specifications

3. **TVRA P**rocess **M**odel to achieve high level security Assurances by recursive application of linear TVRA paths

4. **TVR A**nalysis **L**anguage to specify Security Dependencies (linear path)

5. **TVRA T**ool **B**ox containing 5 generic tools and various concrete tool candidates to instantiate generic tools
   1. Generic tool defines input/output relationship
   2. Concrete tool performs i/o relationship and transforms data

TVRA Information(Tree) Model (1)

- *(ToE_Id:* name, description, purpose, goal, ToE_assumption, ToE_environment, assump_ on_TeE-Env, ToE_details, ***ToE-Interf_Id, Asset_Id, Sec_Obj_Id***)
  - *(ToE_Interf_Id:* name, description)
  - *(Asset_Id:* name, description, category, dependencies, containment)
  - *(Sec_Obj_Id*: category, name, description)

- *(FSR_Id*: name, description, FSR_class, ***Sec_Obj_Id, Component_Ids***)

- *(Abst_CM_Id*: name, description, Risk_Reduction_Value, ***Sec_Obj_Id***, ***CM_family_Id, Weakness_Id***)
  - (CM_Family_Id: name, description, category)
  - (Weakness_Id: name, description, ***Vuln_Id, Threat_Id, Un_Incident_Id***)

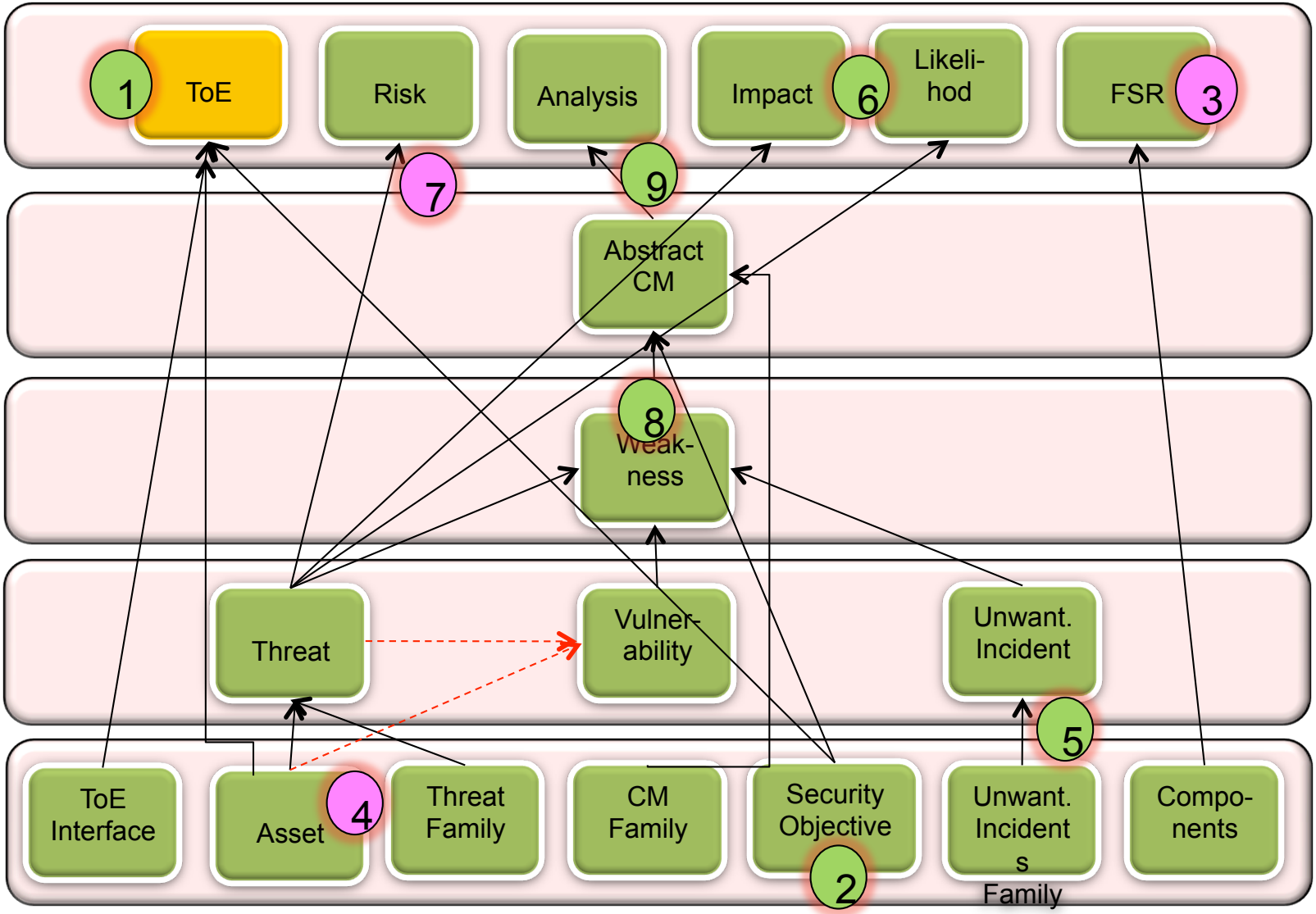
- *(Vuln_Id*: name, description, ***Asset_Id, Threat_Id***)

- *(Threat_Id*: name, description, threat_agents, automated_threat, ***Threat_family_Id, Asset_Id***)
  - *(Threat_Family_Id*: name, description, category)

TVRA Information (Tree) Model(2)

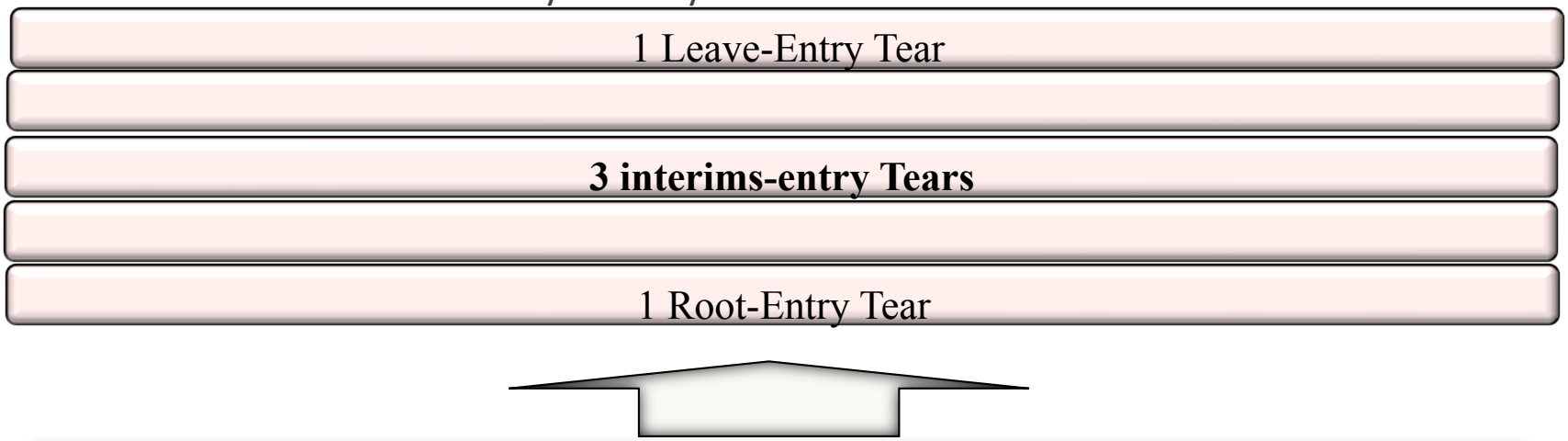
- *(Un_Inc_Id*: name, description, ***Un_Inc_family_Id***)
  - *(Un_Inc_Family_Id*: name, description, category)
- *(Impact_Id*: Asset_Impact, Attack_Intensity, Impact_Value, ***Threat_Id***)
- *(Risk_Id*: Likelihood_Value, Impact_Value, Risk_Value, ***Threat_Id***)
- *(Likelihood_Id*:Time, Expertise, Knowledge, Opportunity, Equipment, Likelihood_Value, ***Threat_ID***)
- *(Analysis_Id*: Standards_Design, Implementation, Operation, Regulatory_Impact, Market_Acceptance, Risk_Reduction_Value, ***Abst_CM_Id***)

SET FW - ETSI TISPAN07/MTS – NGN TVR-Analysis Guidelines (2)



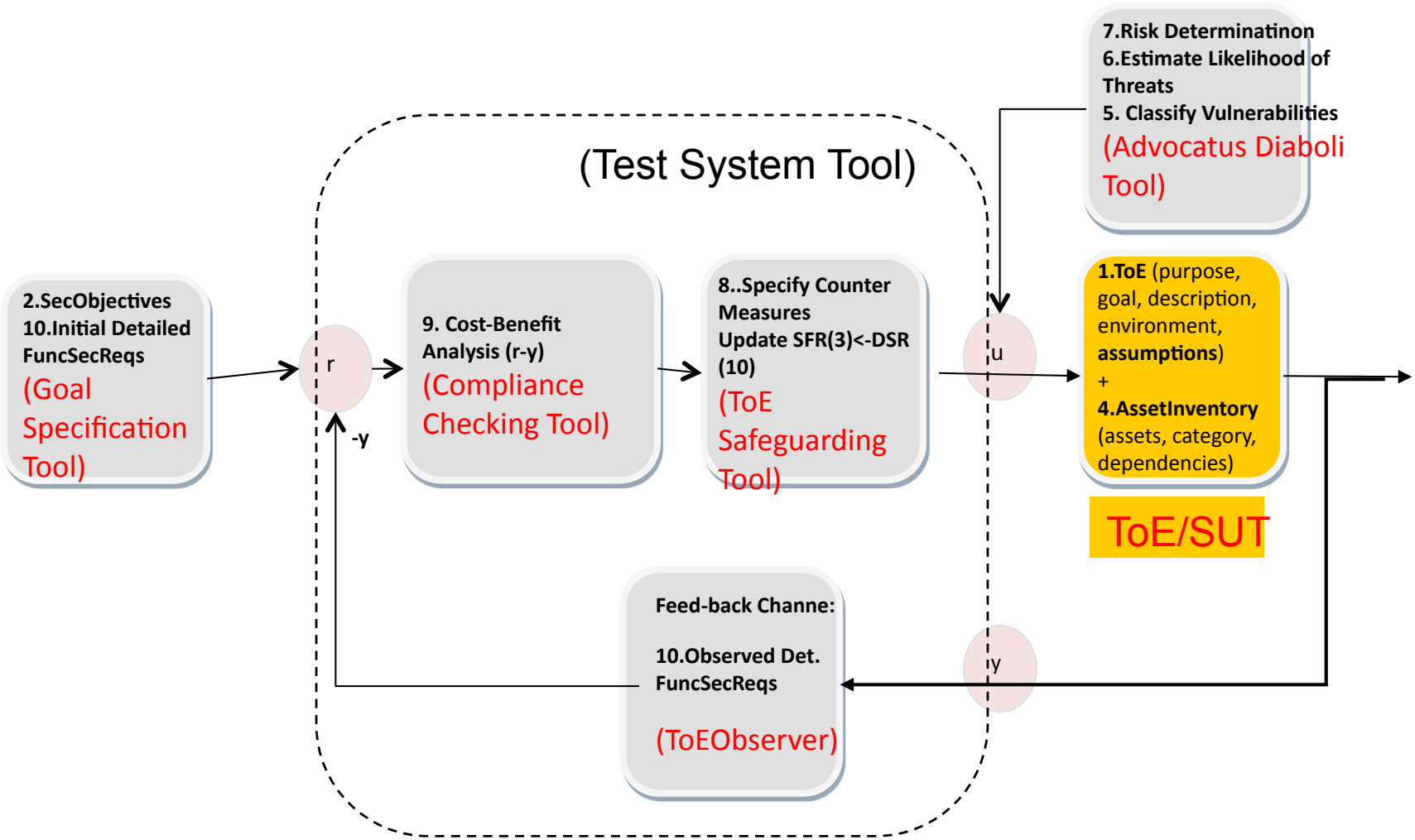
SET FW – TVRA Data Structure Model (4)

- Correctness Criteria:
  - If an entry has null output pointers it is called leave-entry
  - If an entry has null input pointers it is called root-entry
  - If an entry has one or more input and output pointers it is called interims-entry
  - Links must point upward to an entry of a higher tear!
  - To An interims-entry must point one or more input pointers
  - From An interims-entry must point one or more output pointers
  - Root Tear Entries are fed by Security Parameter Definitions



Security Parameter Definition:
Details, Values, Assumptions, Implementation, Equipment, Knowldege, …

SET FW - TVRA Process Model (Security Testing Objectives)



SET FW –
TVRA Process Modell - Toolbox Entries

- **TVRA Toolbox comprises**

  - **5 generic tools**
    - to specify goal requirements,
    - to compare goal requirements with current Trustworthyness QoS of ToE,
    - to make decisions on countermeasure adaptations by analysing identified risks and Vulnerabilities of ToE
    - To disturb a countermeasure‘s effect on ToE (to simulate real attack)
    - To measure current behaviour of ToE and to translate measurements into QoS levels of Trustworthyness

  - the ToE which keeps the assets being safeguarded against any effort of attack

  - Recursive approach to minimize risks of attacks and vulnerabilities of the ToE

SET FW –
TVR ALanguage to Traverse IM Paths(1)

From the „Information Model (3)“ we derive valid TVRA-paths:

- A valid path is a sequence of steps from root entry to a leave entry, without cycles (linear), provided there is no feed-back testing channel tool!
- Alternative paths get connected by logical AND – not OR, because the sum of information which is collected by traversals is entered to the leaves
- Valid paths may start at different roots and end at different leaves, e.g.

1. (CM_Family & *Weakness* -> AbstractCM) -> Analysis[CostBenefit, AbstractCM]
    - (*Threat* & *Vulnerability* & *UnwantedIncident*) -> Weakness
    - (Asset & ThreatFamily) -> Threat
    - (Asset -> Threat) -> Vulnerability

SET FW –
TVRA Language to Traverse IM Paths(2)

- From the „Information Model (3)“ we derive valid TVRA-paths:

  2. (ToE_Interface & Asset & Security_Obj) -> ToE
  3. (Asset -> Threat) -> (Risk & Impact & Likelihood)
  4. Component -> FSR

- The former 4 path/trees define all 6 leave-entries completely wrt

  TVRA, i.e. there is no optional path from roots to leaves!

Conclusion SET FW – Objectives Identification

- **Authenticity**: authentic reference signalling inputs r from BLZ to STWs or engine drivers or OBUs, if necessary by authentication protocols;
  - Prevention of Masquerade attacks
- **Confidentiality**: confidential interaction between **G-** and **H-** institutions, (e.g. OBU, RBC, LEU, Stellwerk, BLZ etc.) in order
  - To prevent Eavesdropping attacks, i.e. all parties need to be legitimated
  - To maintain Privacy of communication that share media with the public domain;
- **Availability**: Enforcement of necessary bandwidth on demand from authorized parties, e.g. to serve signalling (r) or measurement (y) bandwidth demanded by BLZ
- **Integrity**: transmission of steering instructions u and variable measurments y must be safe
  - To prevent compromisation of **u,y** by attackers

Contact:
ETSI TISPAN07 STF415 Expert