ETSI

World Class Standards

SECURITY EVALUATION&TESTING: SET FRAMEWORK

A Contribution to NWI

“MTS Security Design Guide Enabling Test and Assurance”

@ ETSI MTS#55 Meeting, January 24-25, 2012:

Jan deMeer, ssl.eu GmbH Berlin,

(based on contributions to ETSI TISPAN

of 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]

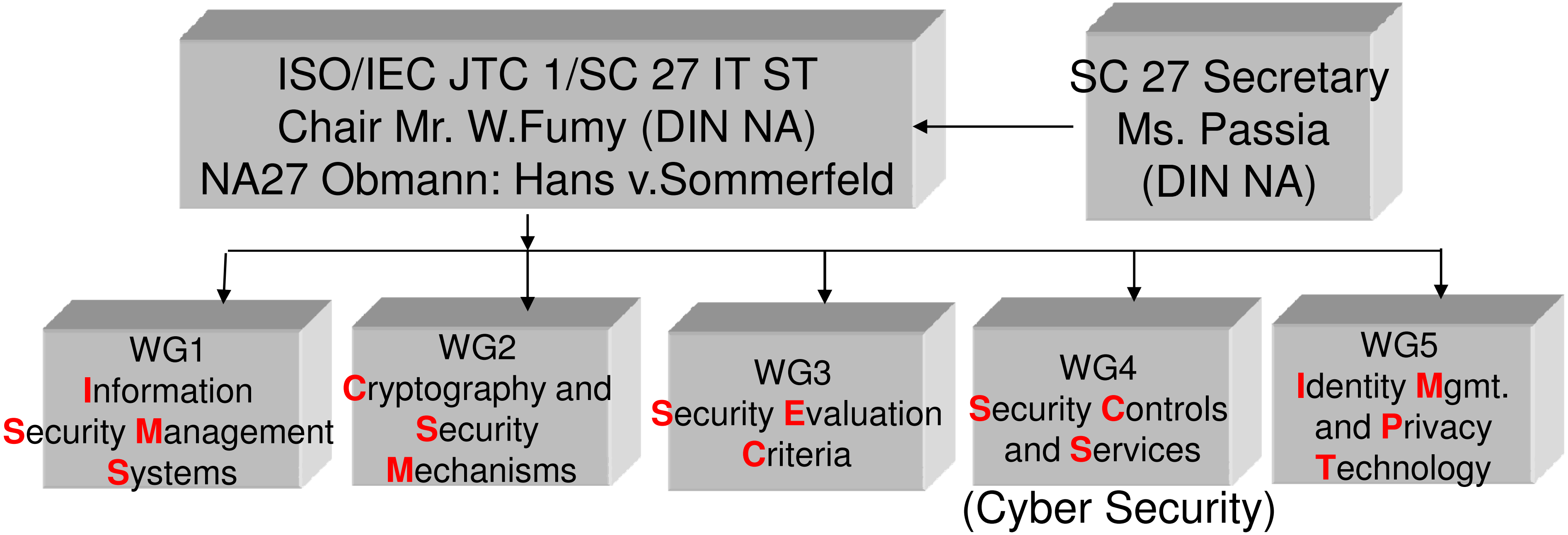
- **ENISA Measurement Frameworks and Metrics**
  - Information Security Metrics
    - Incident – Vulnerability – Patch – Application - Configuration
- **ISO27001/2/4:2009 ISMS**
  - Security Requirements & Security Control Objectives

SET FW - IT Security Technics
DIN NIA27 - ISO/IEC JTC1/SC 27

ISO/IEC JTC1/SC 27 includes

- Identification of Generic Requirements for IT System Security Services
- Specification of Security Guidelines and Security Management Standards
- Specification of Criteria for IT Security Evaluation and Certification
- Development of IT Security Techniques and Mechansims, e.g. Cryptography

DIN NA 043-01 27 AA Normenausschuß: www.ni.din.de



ISO/IEC JTC 1/SC 27 IT ST
Chair Mr. W.Fumy (DIN NA)
NA27 Obmann: Hans v.Sommerfeld

SC 27 Secretary
Ms. Passia
(DIN NA)

WG1
Information
Security Management
Systems

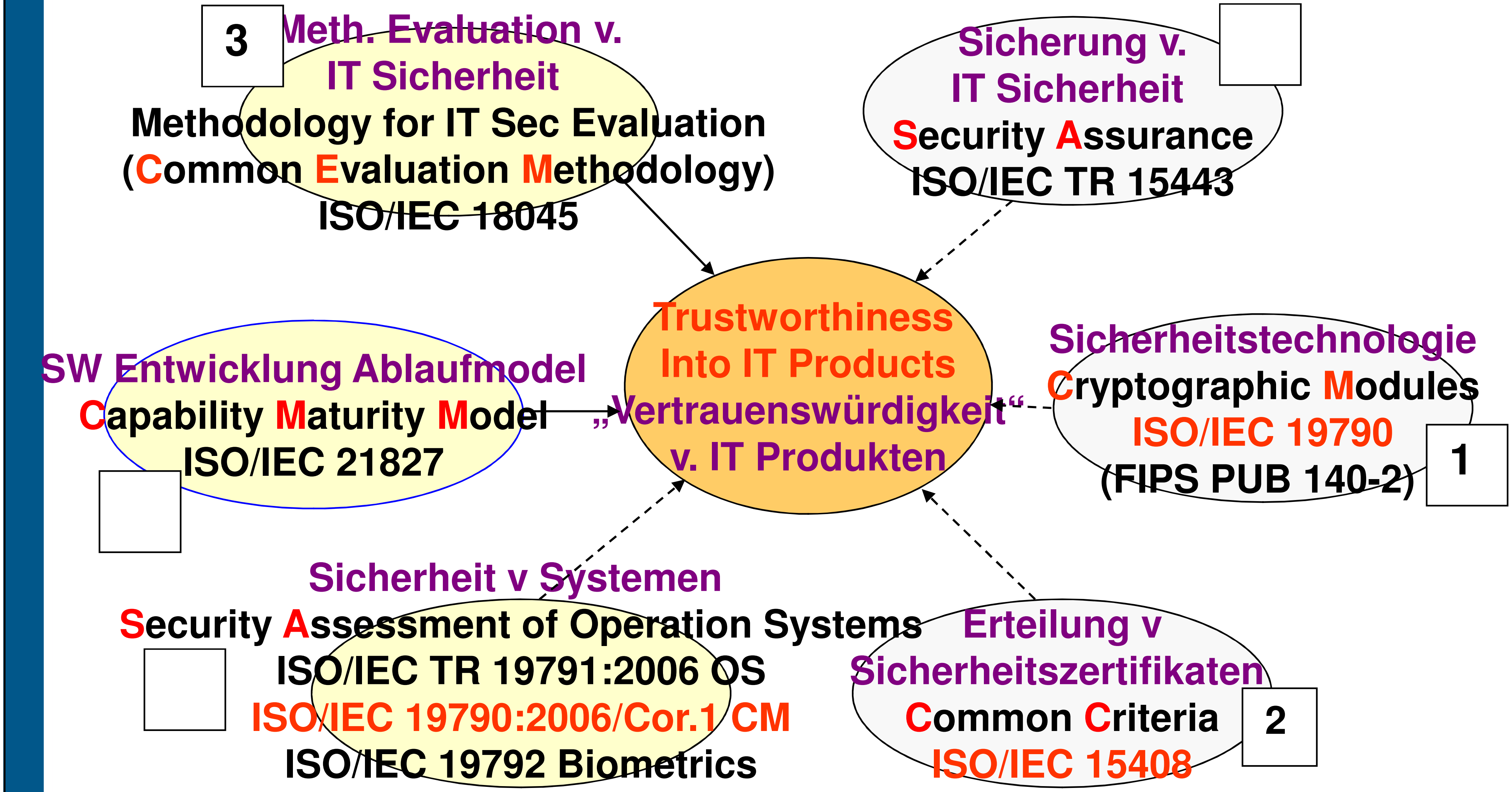
WG2
Cryptography and
Security
Mechanisms

WG3
Security Evaluation
Criteria

WG4
Security Controls
and Services
(Cyber Security)

WG5
Identity Mgmt.
and Privacy
Technology

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



3

Meth. Evaluation v.
IT Sicherheit
Methodology for IT Sec Evaluation
(Common Evaluation Methodology)
ISO/IEC 18045

Sicherung v.
IT Sicherheit
Security Assurance
ISO/IEC TR 15443

SW Entwicklung Ablaufmodel
Capability Maturity Model
ISO/IEC 21827

Trustworthiness
Into IT Products
„Vertrauenswürdigkeit“
v. IT Produkten

Sicherheitstechnologie
Cryptographic Modules
ISO/IEC 19790
(FIPS PUB 140-2)

1

Sicherheit v Systemen
Security Assessment of Operation Systems
ISO/IEC TR 19791:2006 OS
ISO/IEC 19790:2006/Cor.1 CM
ISO/IEC 19792 Biometrics

Erteilung v
Sicherheitszertifikaten
Common Criteria
ISO/IEC 15408

2

SET FW Sources - NGN Security & Resilience Architecture

- **ETSI TISPAN TS 187 001 – NGN Security Requirements*)**
  - stakeholder model with 7 actors
  - 5 Use Cases with respect to Resilience
  - NGN Subsystems
- **(Note: Stage 1 model using use-cases as a tool to illustrate the relationship of stakeholders to the NGN)**

- **ETS TISPAN TS 187 003 – Security Architecture**
  - NGN Security Services
  - NGN Security Domains
  - NGN Security Policies

SET FW Sources:
Resilience Principle?

- System Resilience according to ISO/IEC 27001/2/4
  - **I**nformation **S**ecurity **M**anagement **S**ystems
  - -> CIA Resilience Requirements!
    - **C**onfidentiality to ensure data, services, assets
      - Accessible only by Authorized users
    - **I**ntegrity, i.e. Accuracy, that brings “Completeness” into information Processing
    - **A**vailability to provide access to users being authorized to request assets

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
      - to exclude users from servicing that are not authorized,
      - i.e. To allow only “properly” authorized users to be able to invoke services
    - **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
    - (Note: Prevent-Detect-Correct does not apply only to resilience and in fact the ENISA report does not consider this approach as critical)

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

NGN Stakeholders (= UML Actors)

Security Objectives depend from Stakeholder Roles$^{*)}$

(Note :TS 187 001 does not use this terminology but presents the roles and capabilities per stakeholder in a tabular and graphical form only)

TVRA 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)]

ETSI TISPAN 07 TS 187 001 – NGN Subsystems

NGN Subsystems

NGN consists of subsystems having relations with each other:

[NGNSubsystem ListOf(DirectRelationship) (ListOfStakeholderInteraction)]

[**N**etwork**A**ccess**S**ub**S**ystem (RACS) (EndUser)]

[**R**essource**A**dmission**C**ontrol**S**ubSystem (IMS, RACS) (-)]

[**I**nternet**M**ultimedia**S**ystem (RACS, IMS) (ServiceProvider, EndUser / **IMS P**ublic**U**ser / IMS PI)]

Integrated Assets - Stakeholder Model NGN Resilience Dependencies(3)

All Systems are matters of internal failures and external threats that both interfere with system operation:

Example: Electromagnetic Fields interfere with CPU Operation;

Failures or Threats yield effects on system behaviour dependent from location and component of failure;

The **input signal e** is interferred with **jamming signal n** that both effect **applied system resources (assets) G**:

$$e_1 = G_1 e;$$
$$y' = G_2(e_1+n) \approx G_2 n,\ e_1=0,\ \text{for } H=0;$$
$$y = G_2(e_1+n) = G_2(eG_1+n) = eG_1G_2+nG_2,\ \text{for } H\neq 0;$$
$$y = nG_2 \,/\, (1 + G_1G_2H)$$

Effects of unwanted Threats orFailures can be controlled by the extended **resilience gradient** divisor $(1 + G_1G_2H)$ provided gradient is >1 and system can be stabilized.

SET FW - Integrated Assets-Actors Model NGN Resilience Dependencies(4)

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

diverging results wrongly computed from test/control commands: u->y

Diverging inputs wrongly derived from reference commands r of the model

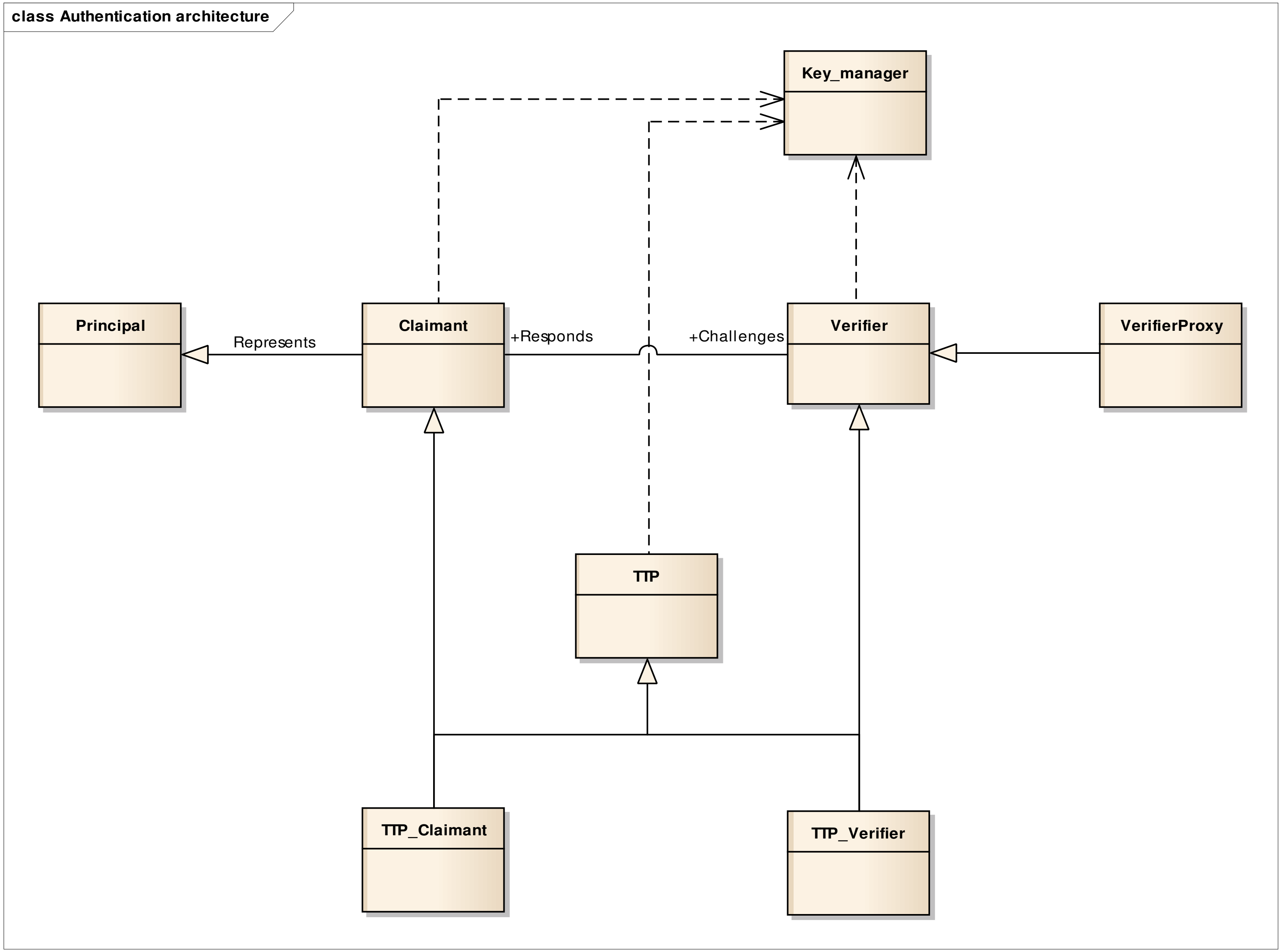
To achieve **System Stability** by providing Activity Control

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



ETSI TS 187 003 v3.4.3 NGN Security Model(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

ETSI TS 187 003 v3.4.3
NGN Challenge-Response Authentication Model(2)

- Challenge-Response Authentication Roles
  - Authentication Association:
    - Claimant by Responds
    - Verifier by Challenges
  - Authentication Role Relationships:
    - Claimant represents Principal
    - Verifier is_assisted_by VerifierProxy
    - (TTP_Claimant TTP_Verifier) act_as TTP
    - TTP_Claimant is_proxy_for Claimant
    - TTP_Verifier is_proxy_for Verifier
  - Authentication Activity Relationships:
    - Claimant is_authenticated_at KeyManager
    - Verifier initiates_authentication_at KeyManager
    - TTP interact_as_proxy_with KeyManager

ETSI TS 187 003 v3.4.3
NGN Challenge-Response Authentication Model(3)

- **Challenge-Response Authentication Assets:**

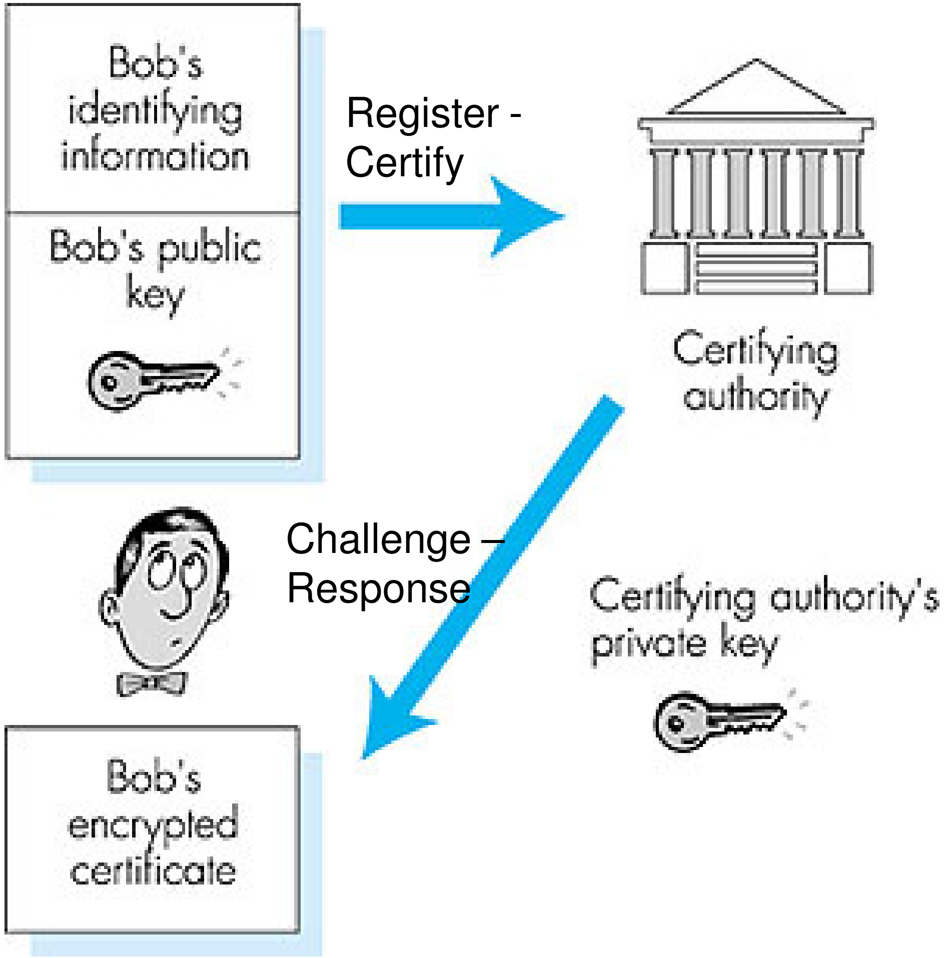
- Certification Authority == Key Manager
- Bob == Principal
- Alice == Verifier, Claimant

- `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`$_B$

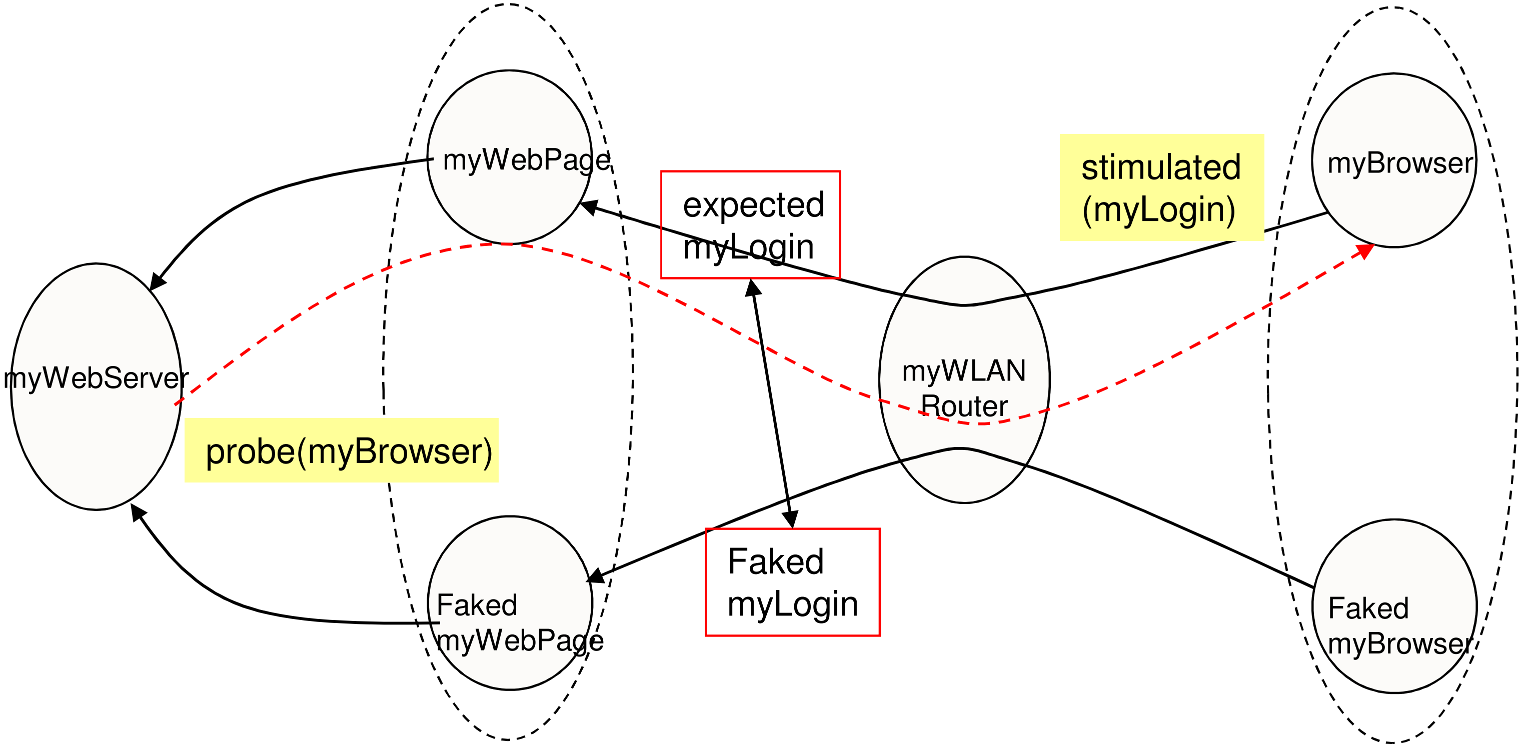
- `Claimant: [IdProofB]`$_A$
- `Response: IdProof`$_B$ `-> PuK`$_B$ `IdInfo`$_B$


Bob's identifying information
Bob's public key
Register - Certify
Certifying authority
Challenge – Response
Certifying authority's private key
Bob's encrypted certificate

Example DNSChanger Trojan Threat – Problem Statement

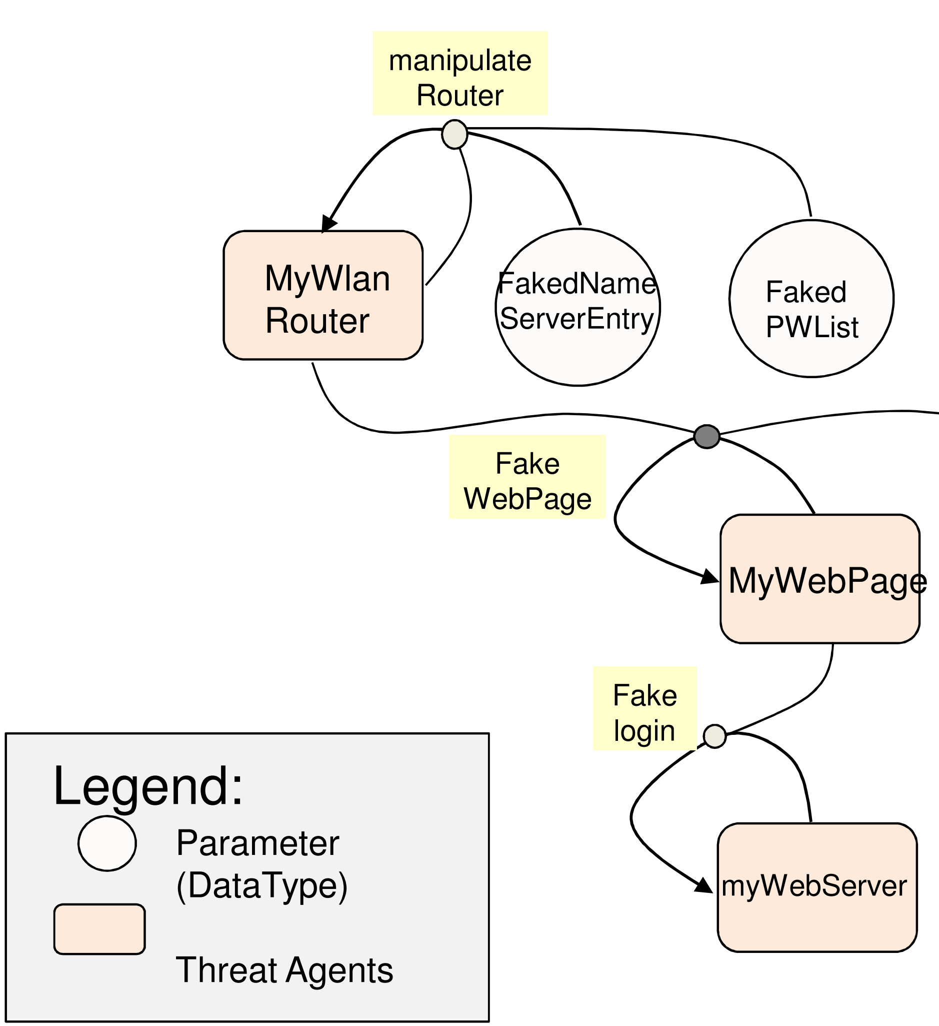
- Attack By Faking `myBrowser` and `myWebPage`:
  - `myBrowser` and `myWebPage` do not longer operating in an authentic manner

  - Question is how to test/check non-authentic operation of components?
    - E.g. Server `probes myBrowser` with a `mylogin` request!
    - If `stimulated mylogin` request gets not redirected, the browser operates authentically!



Example DNSChanger Trojan Threat – Tiers of Attack

- 3-Tier Threat Operational/AgentTopology:



I: tier of Vulnerability Checking

II: tier of faking

III: tier of Threatening

Example DNSChanger Trojan Threat – TVRAnalysis

- TVRA-based Threat Analysis usingThreat Specification Rule:
- *(Threat_Id*: name, description, threat_agents, automated_threat_actions, ***Threat_family_Id, Asset_Id***)
  - *(Threat_Family_Id*: name, description, category)
  - *(Asset_Id:* name, description, category, dependencies, containment)

- *(**Threat_Id***: **DNSChanger**, „fakes Browser and WLAN Router of a User“, (threat_agents: `fakedBrowser, fakedWLanRouter, fakedWebPage`), (threat_actions: `installTrojan, manipulateRouter, fakeWebPage, fakeLogin`), ***Threat_family_Id, Asset_Id***)
  - *(Threat_Family_Id*: Trojan, „inserts ActiveXElement into Browser“, category: repairable)
  - *(Asset_Id:* ServerAssets, „purchased private Assets“, category:private, dependencies:invoked by business cases, containment: faked Business/Use Cases)

Example DNSChanger Trojan Threat – Asset Identification

- DNSC Trojan Threat Algebraic Object Specification includes Actors and Activities:

- Components (Actors):

```
• WlanRouter: [PWL, NSE]
• Browser: [skript]
• WebPage: [skript]
• Server[uid, upw]
• TestAgent [uid, upw, probesList]
```

NSE: Name Server Entry
PWL: PasswordList
UPW: User PW
UID: User Id

- Operations (Activities):

```
• manipulateRouter: myWlanRouter fakedNameServerEntry
  fakedStandardLogins -> myWlanRouter;

• installTrojan: myBrowser activeXElement -> myBrowser;

• fakeWebPage: myWebPage myWlanRouter myBrowser -> myWebPage;

• fakeLogin: myServer fakedWebPage -> myServer;
• expLogin:  myServer myWebPage -> myServer;

• probeBrowser: myBrowser myServer probes -> myBrowser;
```

Example DNSChanger Trojan Threat – Model Derivation, Testing and Checking

- DNSC TrojanThreat Threat (Algebraic) Object :

1. A TAO-derived Model is a valid but unproved TAO term expression that coincides with TAO rules of Components (Actors) and Operations (Actvities) from TVRAnalysis

2. Models with different assumptions (e.g. valid – faked) can be derived from TAO and tested against real System:

- ValidModel: probeBrowser(myBrowserN expLogin(myServerN myWebPageURL) DNSCprobe);

- FakedModel: probeBrowser(myBrowserN fakeLogin(fakedServerN fakedWebPageURL) DNSCprobe);

3. vice versa a (TTCN-3) test trace derived from Real-Time System can be transformed into a model and checked for validity against TAO

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: 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 „closing 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: SET FW Roadmap

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)

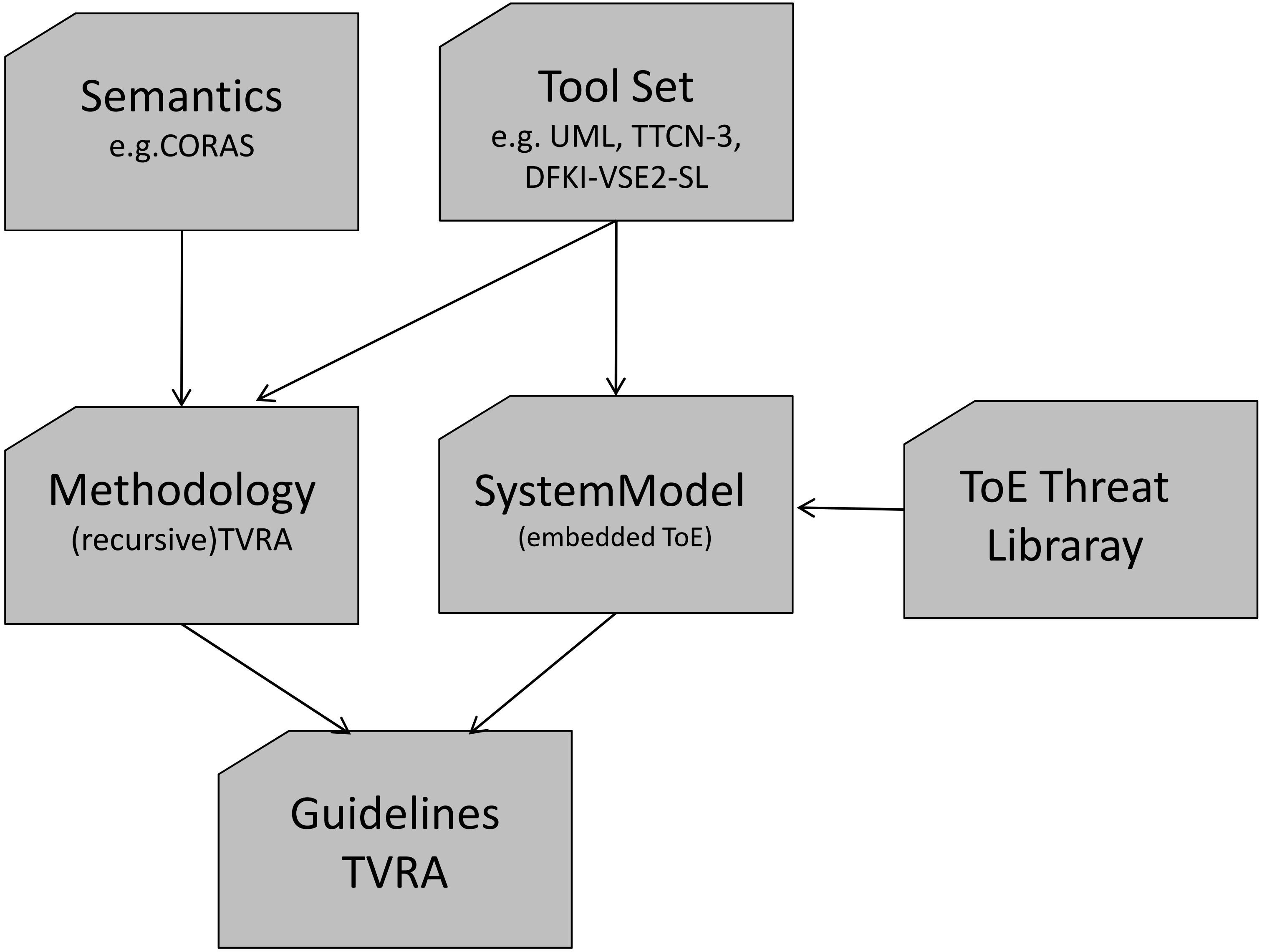
2. identify a Security Evaluation Methodology,
   in terms of Security-related components, i.e. iST, PP, ToE:
   (TVRA Risk Metrics, TVRA Methodology, stencil for ToE, Authorization Model)

3. identify an appropriate Security Evaluation Semantics,
   e.g. CORAS, to make decisions on measurements
   e.g. TAO, to reason about Safety&Security Properties

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 – TVRA Toolbox



TVRA Information 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***)

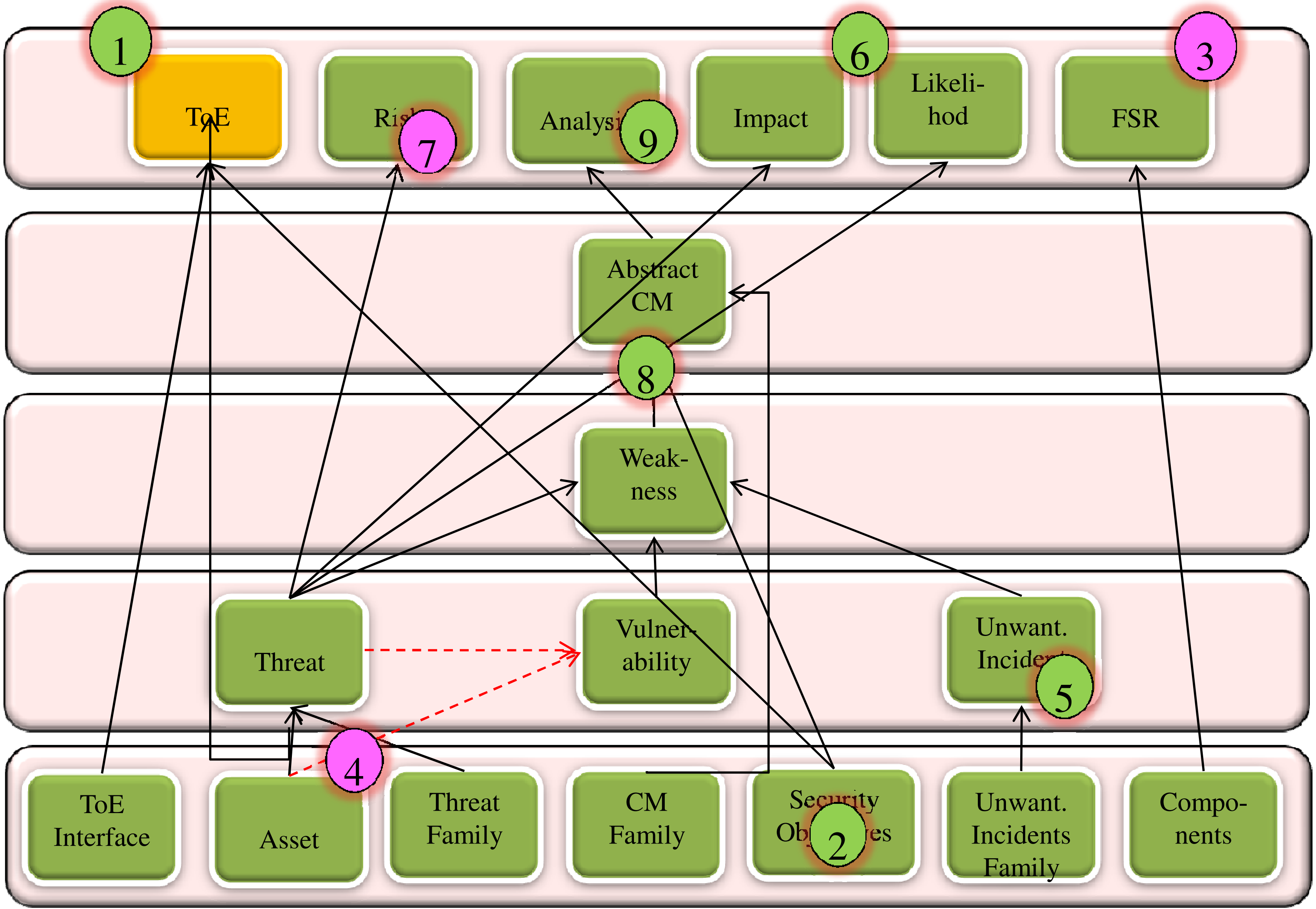
- *(Threat_Id*: name, description, threat_agents, automated_threat, ***Threat_family_Id, Asset_Id***)
  - *(Threat_Family_Id*: name, description, category)

TVRA Information 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***)

Visualization of TVRA Information Model (3)

- TVRA Tree consists of several linked lists of Entries:



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 Trustworthiness
  - 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 - Toolbox Entries: MB Testing vc. MB (TVR)Analysis?

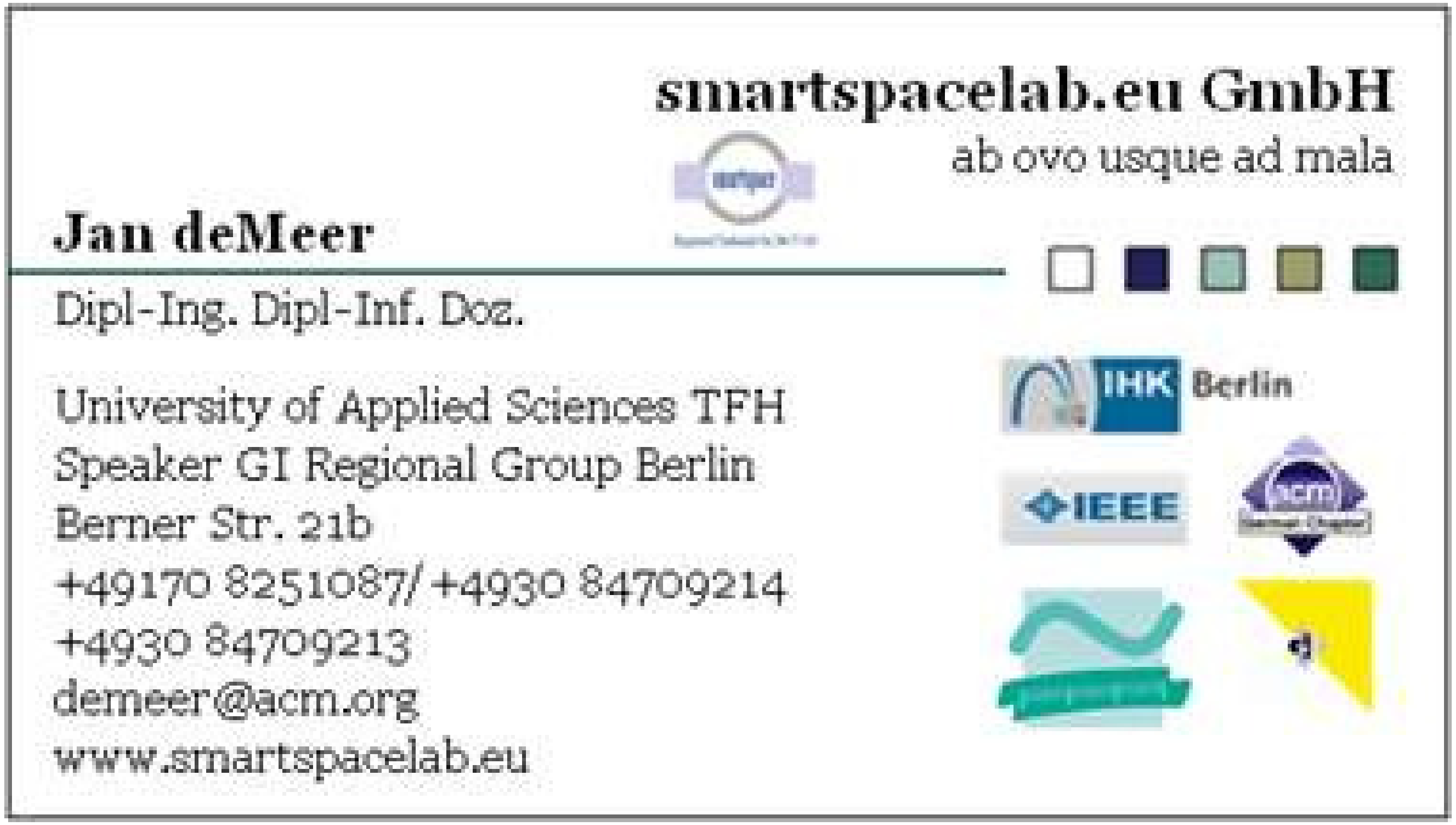
MB Testing = Interative Approach :=

1. to model (Initial) System Design Requirements and Objectives;
2. To derive test cases (probes & effects) from Model;
3. To execute probes and observe their effects;
4. To decide on Validity (pass, fail, inconclusive) of observed probe effects;
5. goto step 2: (to Derive next test case);

MB Analysis = Recursive Approach :=

1. To model (Final) System Application Goals, i.e. Business Objectives: (r);
2. To compare preceding (measured) System State with current (derived) Model State: (r~y‘);
3. Due to (r~y‘) comparision - decide on next test case (probes & effects) and feed them into system: (u);
4. To measure current System State y, as an effect of current probes;
5. To feed-back measured system state to System Model in order to perform next test case computation

Contact:
ETSI TISPAN07 STF415 Expert



smartspacelab.eu GmbH
ab ovo usque ad mala

Jan deMeer

Dipl-Ing. Dipl-Inf. Doz.

University of Applied Sciences TFH
Speaker GI Regional Group Berlin
Berner Str. 21b
+49170 8251087/ +4930 84709214
+4930 84709213
demeer@acm.org
www.smartspacelab.eu

IHK Berlin
IEEE
acm