World Class Standards

TISPAN NGN Security standards

NGN R2 and beyond

Judith E. Y. Rossebø
ETSI TISPAN WG7 Chairman
Telenor R&I

3rd ETSI Security Workshop

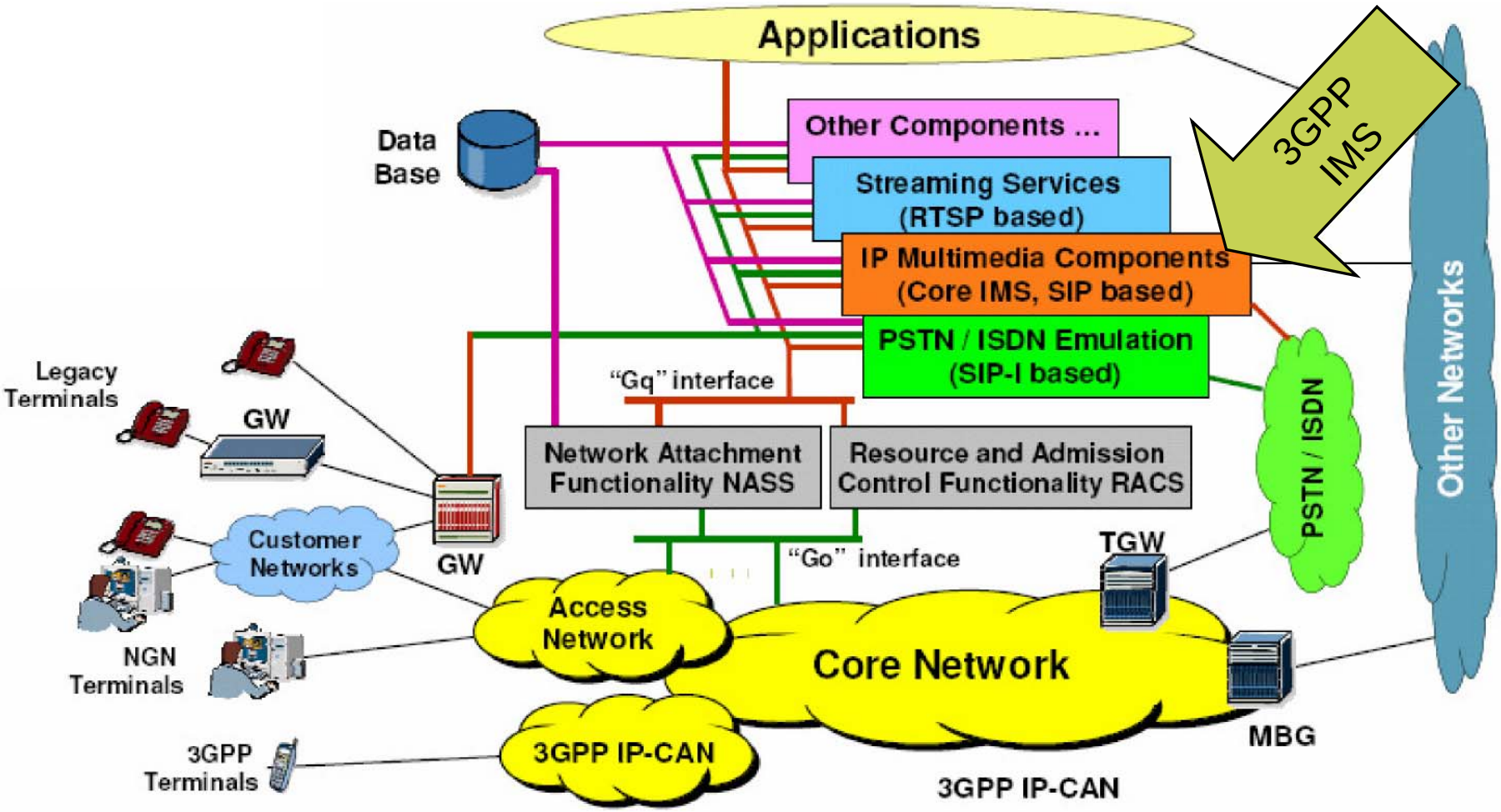
Background

TISPAN NGN

- ETSI TISPAN proposes an architecture basis consisting of a range of subsystems:
  - Access network attachment subsystem (NASS)
  - Resource and admission control sub-system (RACS)
  - PSTN-ISDN emulation subsystem (PES)
  - IP Multimedia Subsystem (IMS) (3GPP)
  - IPTV Subsystem
- TISPAN is adopting standards from other bodies where appropriate
  - Aspects relating to common IMS are not standardized by TISPAN, but if identified shall be transferred to the responsibility of 3GPP

Telecommunication and Internet converged Services and Protocols for Advanced Networking

TISPAN NGN Architecture



TISPAN NGN R1 security:

- NGN Security requirements (TS 187 001)
- NGN eTVRA (TR 187 002)
  - Threat and risk analyses for specific NGN use cases
- NGN Security architecture (TS 187 003)
- NGN Lawful Interception functional entities, information flow and reference points (TS 187 005)

TISPAN NGN R2 security standards

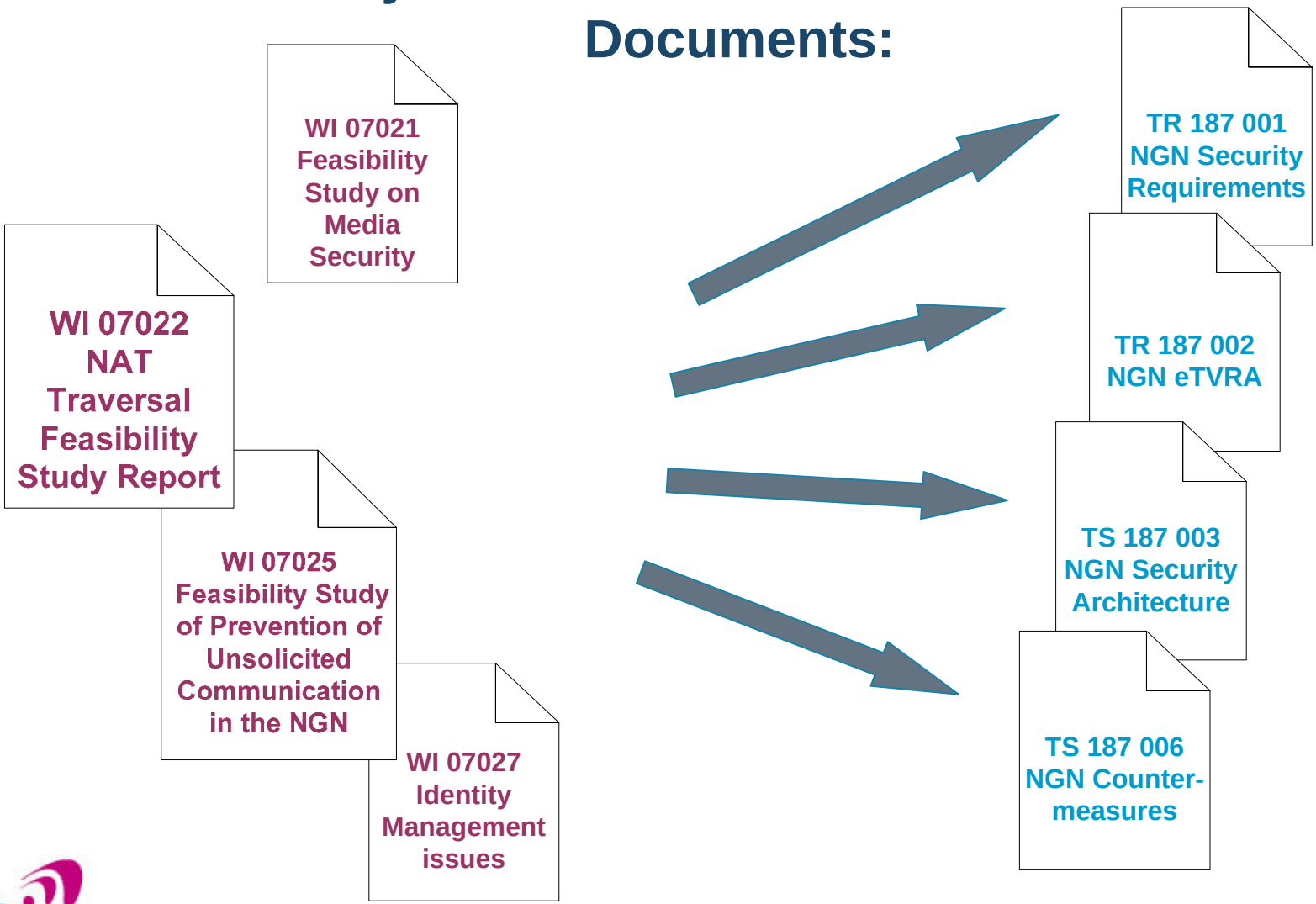
TISPAN NGN R2 security (1/2):

- NGN Security requirements (TS 187 001)
  - Builds on the R1 version of the TS
  - Defines also security requirements for IPTV, Business Communication, Media Security, Home Networking, and for countering UC
- NGN eTVRA (TR 187 002)
  - Threat and risk analyses for specific NGN use cases such as NAT traversal, RACS, Media Security, and Unsolicited Communication;
- NGN Security architecture (TS 187 003)
  - Work is ongoing on defining the security architecture for IPTV, Home Networking, FMC, Media Security, H.248, Corporate Networks
- NGN Lawful Interception functional entities, information flow and reference points (TS 187 005)
  - Builds on the R1 version of the TR

TISPAN NGN R2 security (2/2):

- Generalized NAT traversal feasibility study (TR 187 007)
  - TB approved December, 2007
- Media security (TR 187 008)
- Impact of unsolicited communication in the NGN
- New work item on data retention and its impact on the NGN

NGN Feasibility Studies Feed into TISPAN Core Security Documents:



WI 07025 on Prevention of UC in the NGN

- High level analysis of the impact of prevention of unsolicited communication in the NGN.
- Focus is on unsolicited communication within voice-media (SPIT - voice SPAM)
- Reports on the feasibility of counteracting the occurrence of Unsolicited Communications (UC) in the NGN.
- The report provides a TVRA
  - quantifies the likelihood and impact of UC in the NGN where UC is initiated in a variety of forms.
- It also addresses methodologies for preventing the terminating party from receiving UC.

- Relevant objectives and requirements are extracted for the NGN architecture, signalling and security.

Role of STFs in ETSI TISPAN WG7

Role of STFs in ETSI TISPAN WG7

- **Security standardisation methods and security guidelines**
  - Introduce assurance rigour to standardisation based on the Common Criteria for IT security evaluation (ISO/IEC 15408)
  - Provide guidance to standards developers on standards preparation
    - To allow evaluation
    - To achieve higher quality standards
- **Standards development**
  - Assisting TISPAN WG7 in applying the methods and guidelines developed to NGN R1 and R2 standards development
    - Contributions based on the methods being developed by STF 329 have been provided to the IPTV, NAT-T, RACS, Media Sec, UC prevention and NGN-R2 requirements work items

Current and previous TISPAN security STFs funded by ETSI and EC/EFTA:

STF292, STF316, STF329, STF330, and STF 341

http://portal.etsi.org/stfs/process/home.asp

*e*TVRA

- Threat Vulnerability Risk Assessment funded by *e*Europe
- ETSI STF 292 created TVRA method and tool
  - Under supervision of TISPAN WG7
- Systematic Approach to Risk analysis
  - Systematic Identification of assets and threats and weaknesses, computes a weighted risk level.
- Applicable during:
  - Standards development
  - Development
  - Deployment
  - Utilization
- Tested on analysis for SIP & ENUM

Understanding of security

- **A** Threat, **enacted by a** Threat Agent**, may lead to an** Unwanted Incident **breaking certain pre-defined** security objectives
- **Aim is to avoid** Unwanted Incidents
- **Countermeasures restrict the ability of** threat agents **to operate**

Threat Vulnerability Risk Assessment

0. Identification of the target space
1. Systematic identification of the objectives
   - resulting in a high level statement of the security aims and issues to be resolved
2. Systematic identification of the requirements
   - derived from the objectives given in step 1
3. Systematic Inventory of the assets and their importance
4. Identification and classification of vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that can result
5. Quantifying the occurrence likelihood and the impact of the threats
   - Metrics derived from ETR 332 and ISO/IEC 15408-1
6. Quantifying the risks
   - Uniform comparison of the risk associated with each of the vulnerabilities
7. Identification of countermeasures

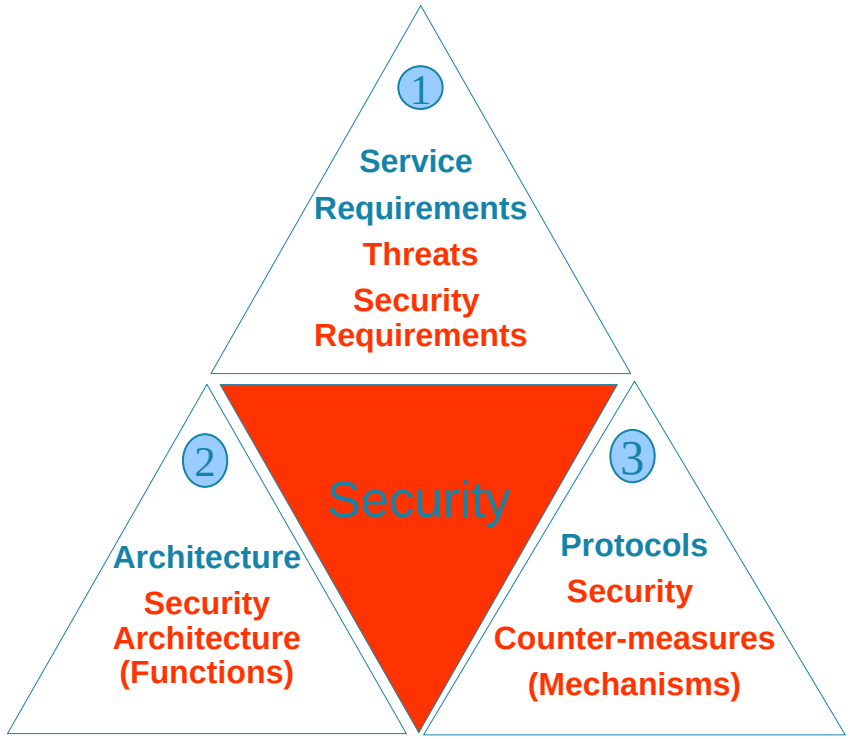
Use of the methods developed by STF292 and STF 329 for IPTV security requirements engineering

World Class Standards

IPTV-Security Requirement Approach.

Development of IPTV-building blocks.

- Analyze IPTV services. Based on this analysis, design an appropriate security model.
  - Based on Service requirements*, identify security objectives and threats and from that deduce security requirements
  - Define security architecture taking into account service and security requirements
  - Develop appropriate countermeasures as re-useable building blocks



* References:

ETSI TS 181 016. TISPAN; Service Layer Requirements to Integrate NGN Services and IPTV.
ATIS. IPTV DRM Interoperability Requirements. ATIS-0800001.
ATIS. IPTV Architecture Requirements. ATIS-0800002.

IPTV-Security Approach.

Development of security building blocks for TISPAN's IPTV.

	Proposed Action		Expected Results
Step 1	▪ Define security objectives for IPTV. Perform TVRA for IPTV service. *This is done based on among other things existing service requirements*	Output	▪ IPTV Security Objectives. Overview of threats related to every single service requirement
Step 2	▪ Deduce security requirements from service profiles and the identified threats.	Output	▪ List of Security Requirements matched to Network and service Layers
Step 3	▪ Put the Security Requirements into relationship to the TISPAN NGN - Model	Output	▪ Overview of Security Services, proposed for IPTV in context of TISPAN NGN
Step 4	▪ Development of suitable Security architecture with adequate security services and their Integration into TISPAN's Architecture	Output	▪ Integration of Security services as reusable building blocks to the overall NGN-Architecture ▪ Harmonization with existing Protocols

World Class Standards

IPTV-Security Approach : Brainstorming phase

Service requirements to Security requirements mapping

	Service Requirements	Security Threats	Initial Security Requirements/Initial Countermeasures
5.1.1	The IPTV solution shall support the individual addressability of devices acting as UEs located in the Consumer Network.	Device Address manipulation, masquerading, theft of service.	Implicite device authentication with temper-proofed certificates
5.1.2	One user can access a service through multiple UEs simultaneously.	Device Address manipulation, masquerading, theft of service.	Session key supported by multiple UE s. Prior to the IPTV access, every single UE must be implicit authenticated.
5.1.3	One user can access multiple services through an UE simultaneously.	Masquerading, theft of service, IP-Spoofing.	One UE must offer authorized access to multiple services. To use one service, user must authenticate and authorize.
5.1.4	The interactive IPTV solution shall be an open solution, that is Operators and Service Providers shall be able to create new service logics that involve both multimedia and communication features.	Device Address manipulation, masquerading, service profiling, theft of device of the multimedia application and masquerading, eavesdropping, data manipulation, privacy violation, espionage, etc. for communication services	Different levels of user authentication and authorization must be supported according to service's threat level.
5.1.5	The interactive IPTV solution shall support downloading service logics on the end-devices (for example via Open API on the STB).	Manipulation of Data, Viruses and Trojans can be delivered	The downloading entity must be authenticated and authorized by the user or user's device. It must be guaranteed that the downloaded data are the original data and their integrity is not violated.
5.1.6	To allow for integrated service logics, the IPTV solution shall have the ability to authenticate the user not just the device.	Masquerading	Mutual authentication between the User and the IPTV service must be supported.

Resulting IPTV security requirements:

(R-IPTV-CN-1)	The NGN R2 IPTV service shall assign unique identities to all IPTV content that are verifiable for users, named groups of users, entities acting on behalf of users and entities acting on behalf of named groups of users
(R-IPTV-CN-2)	The NGN R2 IPTV service shall assign non-forgeable identities to all IPTV content that are verifiable for users, named groups of users, entities acting on behalf of users and entities acting on behalf of named groups of users
(R-IPTV-CN-3)	The NGN R2 IPTV service shall authenticate and authorise all IPTV content to the receiving user, named group of users, entities acting on behalf of a user, and entities acting on behalf of named group of users
(R-IPTV-CN-4)	The NGN R2 IPTV service shall verify the authenticity of all IPTV content to the receiving user, named group of users, entities acting on behalf of a user, and entities acting on behalf of named group of users
(R-IPTV-CN-5)	The NGN R2 IPTV service shall assign unique identities to the origin of all IPTV content that are verifiable for users, named groups of users, entities acting on behalf of users and entities acting on behalf of named groups of users

For the complete list : RTS 187 001 (NGN Security requirements for Release 2)

IPTV security requirements were used to derive the elementary functions required in the IPTV architecture:

- **For content security the following elementary functions are used:**
  - Content licensing: This elementary function handles the licenses issuing related functions, including generation and distribution of the licenses to the desired entities.
    - *From the requirements R-IPTV-CN-1, R-IPTV-CN-2, R-IPTV-CN-3, R-IPTV-CN-4, R-IPTV-CN-5, R-IPTV-CN-6, …, R-IPTV-CN-13, we can see that a licensing related element function is need.*
  - Key management: This elementary function handles the management of the security keys, including generate and provide the keys and corresponding parameters to the desired entities.
    - *From the requirements R-IPTV-CN-1, R-IPTV-CN-2, R-IPTV-CN-3, R-IPTV-CN-4, R-IPTV-CN-6, …, R-IPTV-CN-13, we can see that a corresponding key management element functions is needed.*
  - Content encryption: This elementary function handles the content protection related operations, e.g. content encryption and encapsulation operations etc.
    - *From the requirements R-IPTV-CN-3, R-IPTV-CN-4, R-IPTV-CN-7, …, R-IPTV-CN-13, we can see that an element function is needed to perform the content protection related operations.*

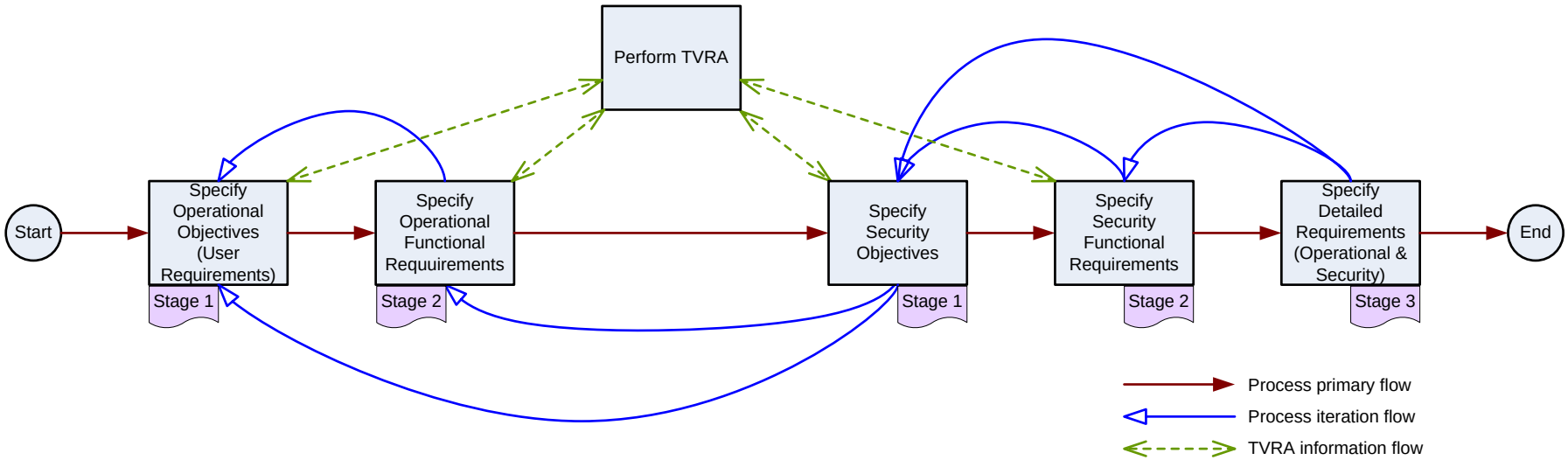
STF 329 - requirements engineering

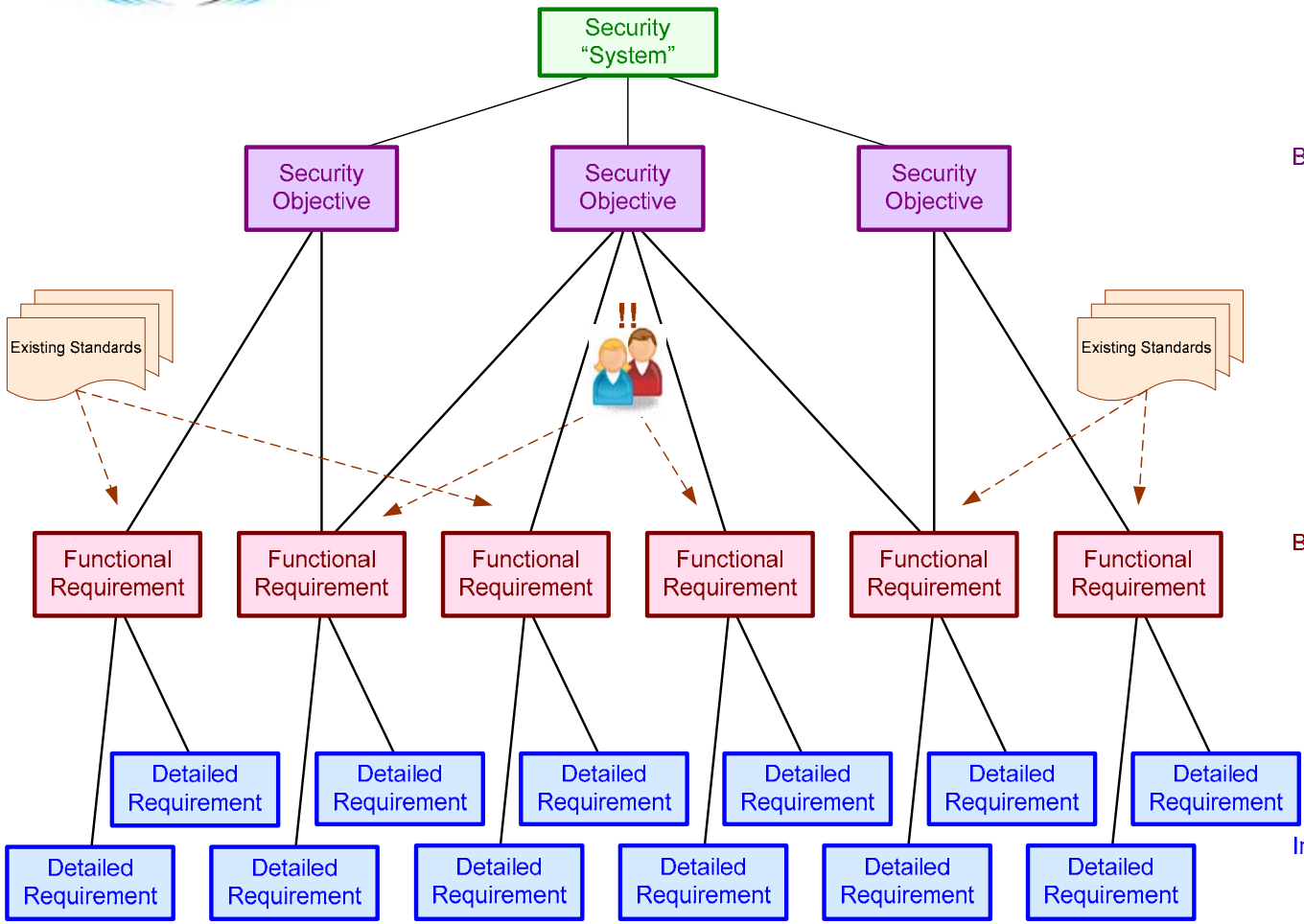
Application of ISO-15408-2 requirements to ETSI standards

- Defines a method, based on the application of ISO 15408-2, for concisely and unambiguously declaring security requirements expressed in ETSI standards.
- The purpose is to provide support to developers of ETSI standards in using the security functional components of ISO 15408-2.
  - In particular it explains the elements in the ISO 15408 2 functional capabilities and describes how they fit within a structured security requirements engineering method.
  - Required elements are defined with respect to the NGN and, where appropriate, are illustrated with examples from the NGN Security programme.

Process for Security Standardization

- Threat, Vulnerability and Risk Analysis (TVRA) is essential
  - For identifying and specifying objectives and requirements
- TVRA is iterated at stages 1, 2 and 3 of the process
  - 3-stage process defined in ITU-T Recommendation I.130





Broad Intentions (What):
- Realistic
- Achievable
- Measurable
- Relevant

Behavioural Building Blocks:
- New and/or existing features
- Act together to meet the defined Objective(s)
- May relate to more than one Objective

Implementation Details (How):
- Atomic
- Structured:
  - Preconditions
  - Stimulus
  - Response
- Categorized:
  - Mandatory
  - Recommended
  - Optional

Hot topics for future work

Topics for future work

- **TISPAN NGN security beyond Release 2**
  - IPTV security (enhancement of stage 2, definition of stage 3)
  - Adding UC prevention as a feature (stage 1, stage 2, stage 3)
  - Media security provisioning (stage 1, stage2)
  - Additional work on NAT-T (e.g. interaction with RACS, interaction with IPTV, security analysis of use of STUN)
  - Enhanced security for NASS, RACS
  - Security for CNG/CND (stage 1, stage 2, stage 3)
    - Implications for AGCF security
  - Security for NGCN
  - FMC (taking into account requirements of the FMCA)
  - Diameter and Radius AVP profiling
  - Application layer security on the NGN (e.g. TELCO 2.0)
  - Analyse the inter-relation between security features and architecture of the NGN (IPTV, NAT-T, NASS, RACS etc.) in terms of how to employ consistent security architecture and mechanisms
    - Develop general rules, patterns, and templates to ease the employment of the NGN in practice and to facilitate risk control

THANKS FOR YOUR ATTENTION

ETSI TISPAN Portal:

http://portal.etsi.org/Portal_Common/home.asp

For more information

- European Telecommunication Standardisation Institute
  www.etsi.org
- TISPAN security specialist task force leader
  scott.cadzow@etsi.org
- TISPAN security working group chair
  judith.rossebo@telenor.com

Navigating the TISPAN security documents

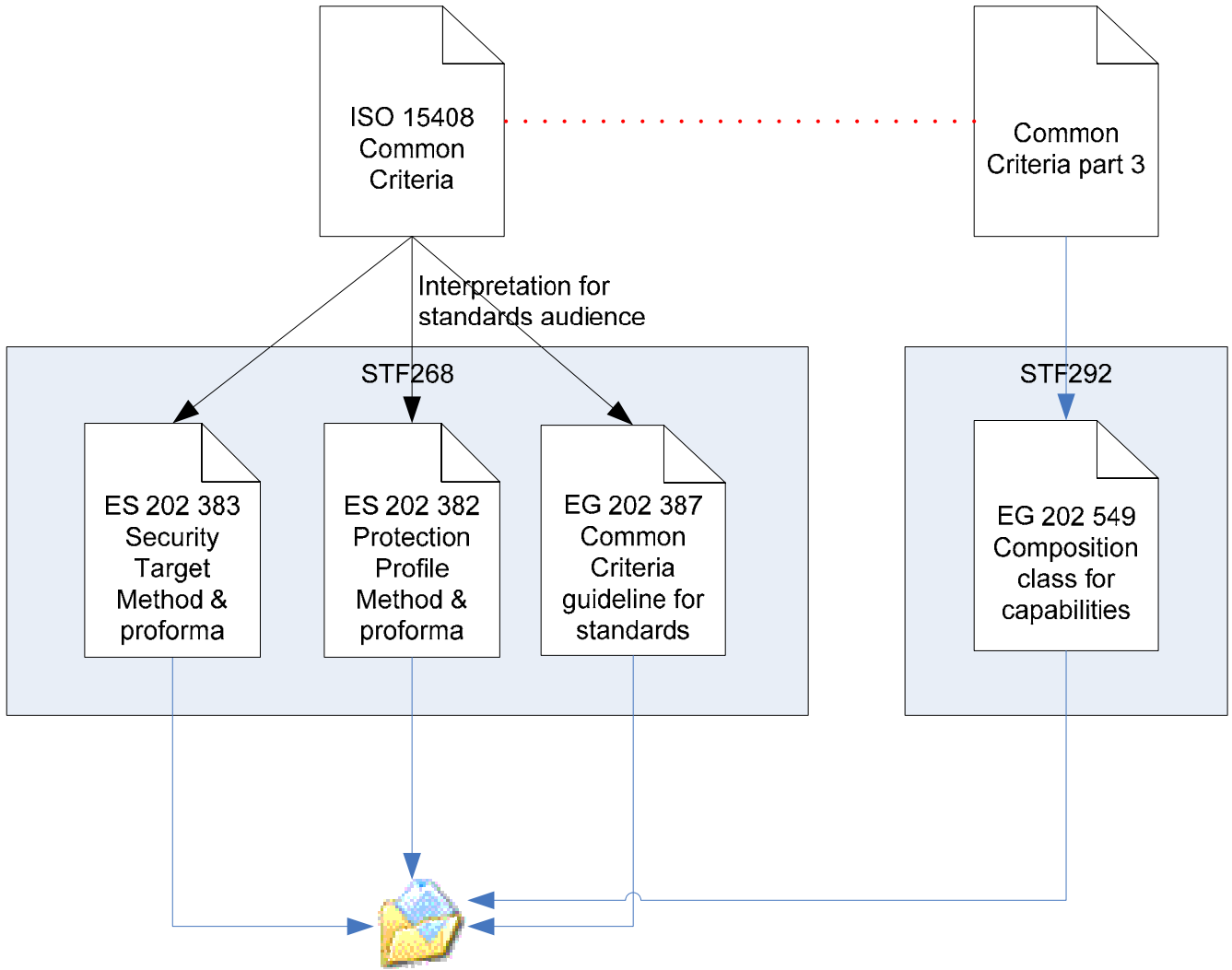
Families of documents #1

- ETSI Common Criteria Guidance documents
  - EG 202 387 (Guide to CC for standards developers)
  - ES 202 382 (PP method and proforma)
  - ES 202 383 (ST method and proforma)
  - EG 202 549 (Design Guide; Application of security countermeasures to service capabilities)
  - WI 07028 Method for application of ISO 15408-2 to requirements specification in NGN
- ETSI Security Standardisation guidance documents
  - ETSI Common Criteria Guidance documents
  - TS 102 165-1:2006 (eTVRA)
  - ETR 332 (obsoleted by eTVRA)
- ETSI Security standardisation method documents
  - ETSI Security Standardisation guidance documents
  - ISO methods and frameworks
  - TS 102 165-2:2006

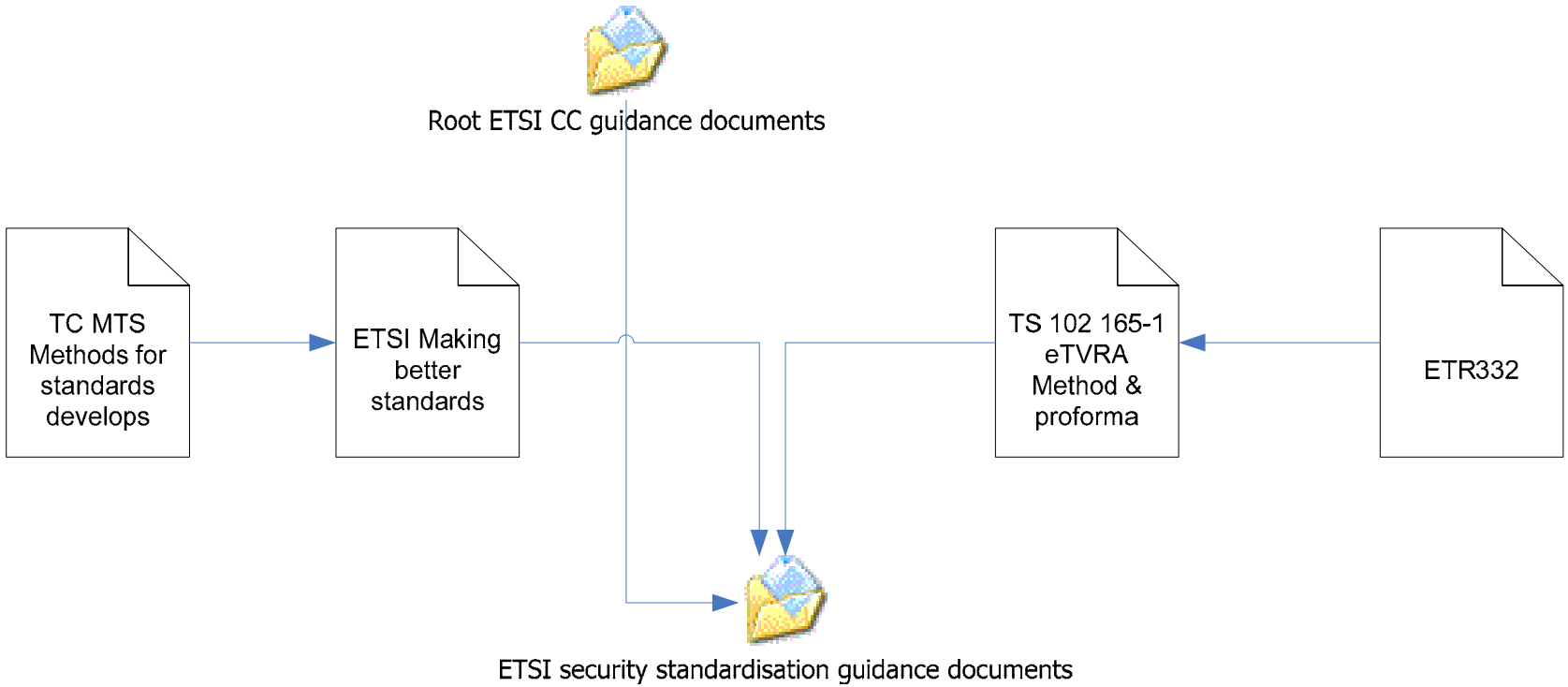
Families of documents #2

- NGN security requirements analysis
  - TR 187 007, NAT traversal
  - TS 187 008, Media security
  - STF-330 output (Identity analysis)
- NGN Security documents
  - NGN security requirements analysis
  - TR 187 001 (NGN Security requirements)
  - TS 187 002 (NGN eTVRA)
  - TS 187 003 (NGN Security architecture)
  - TS 187 006 (NGN Security countermeasures)
  - …

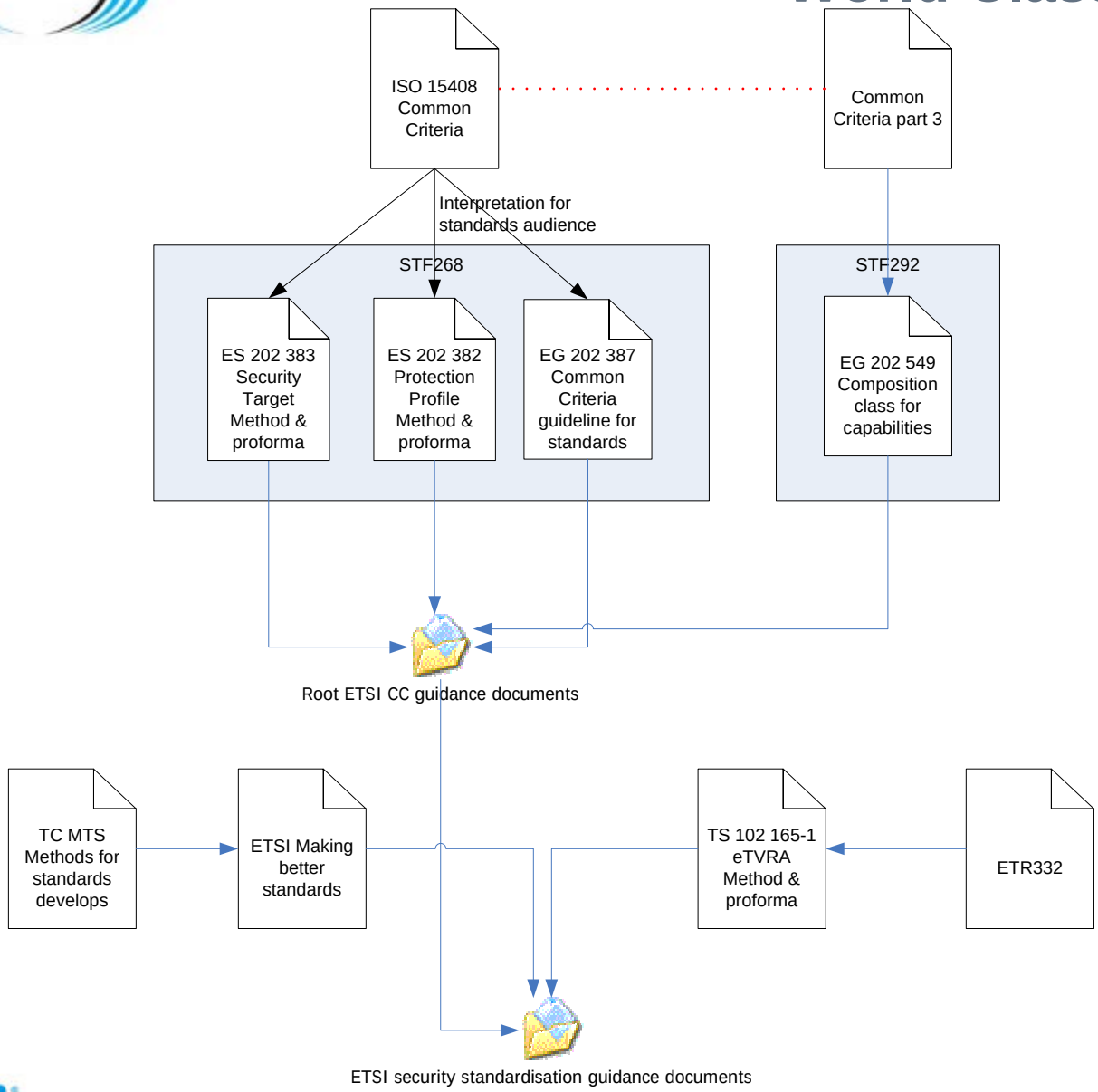
ETSI Common Criteria Guidance documents



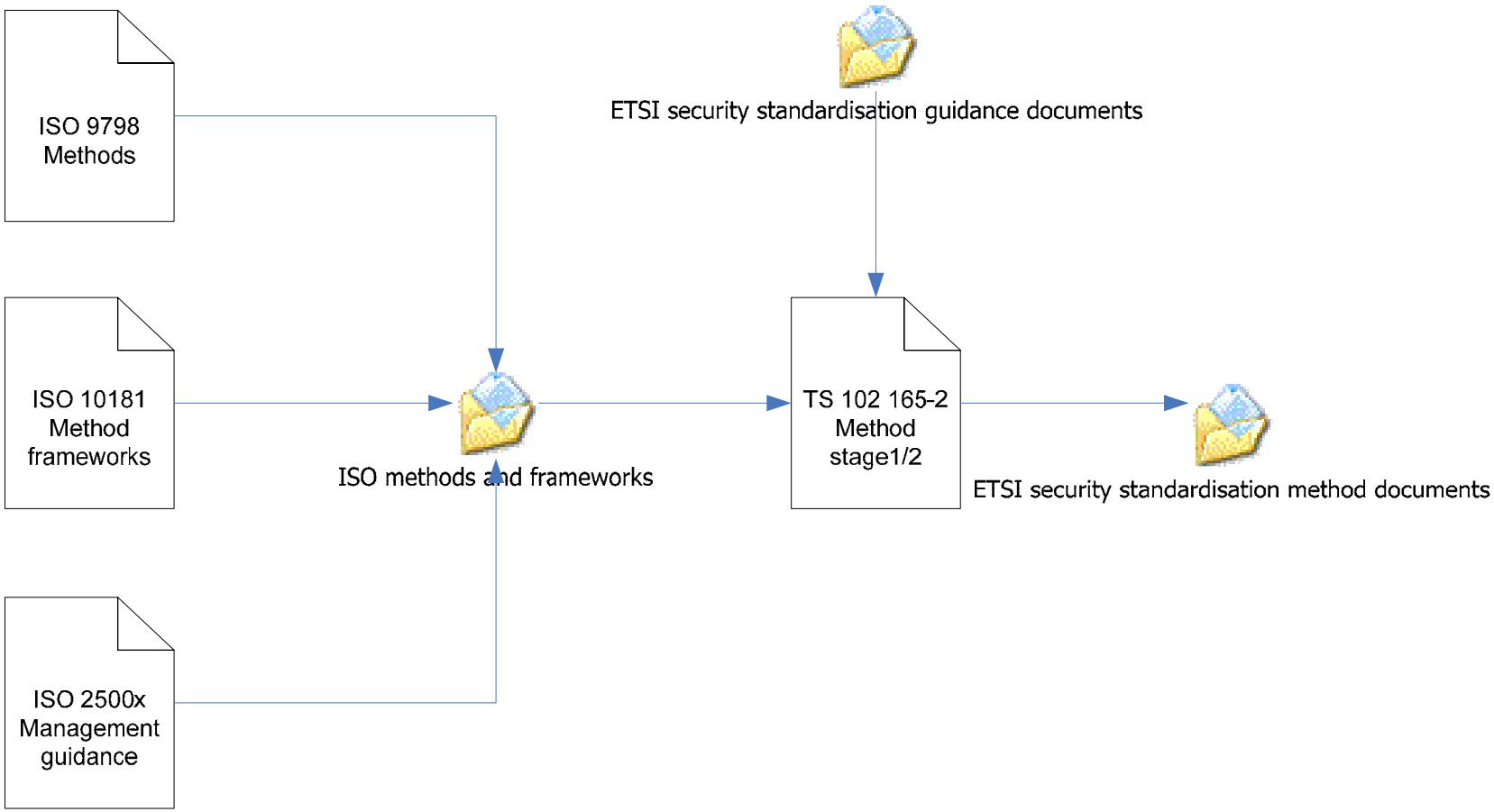
ETSI Security Standardisation guidance documents



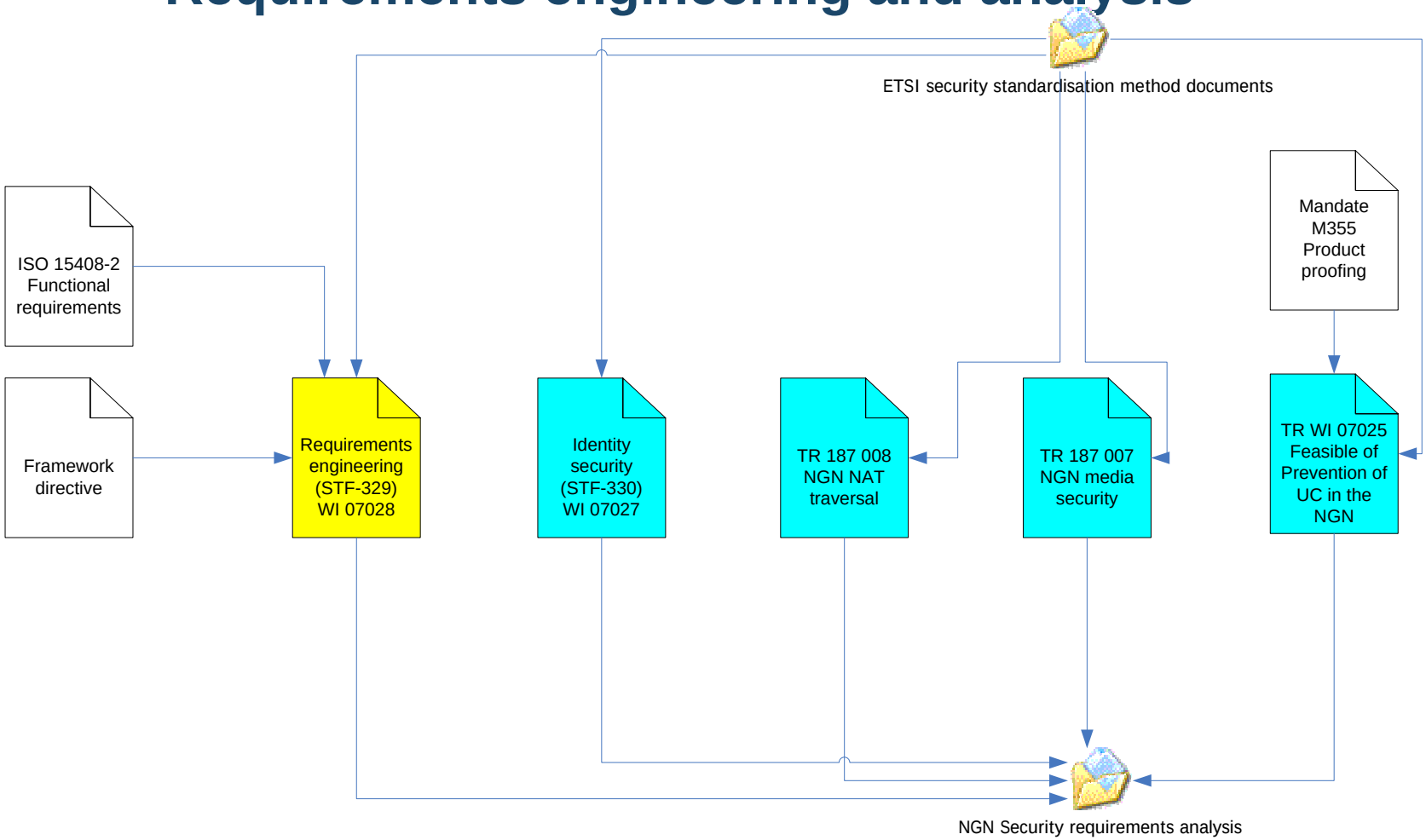
World Class Standards



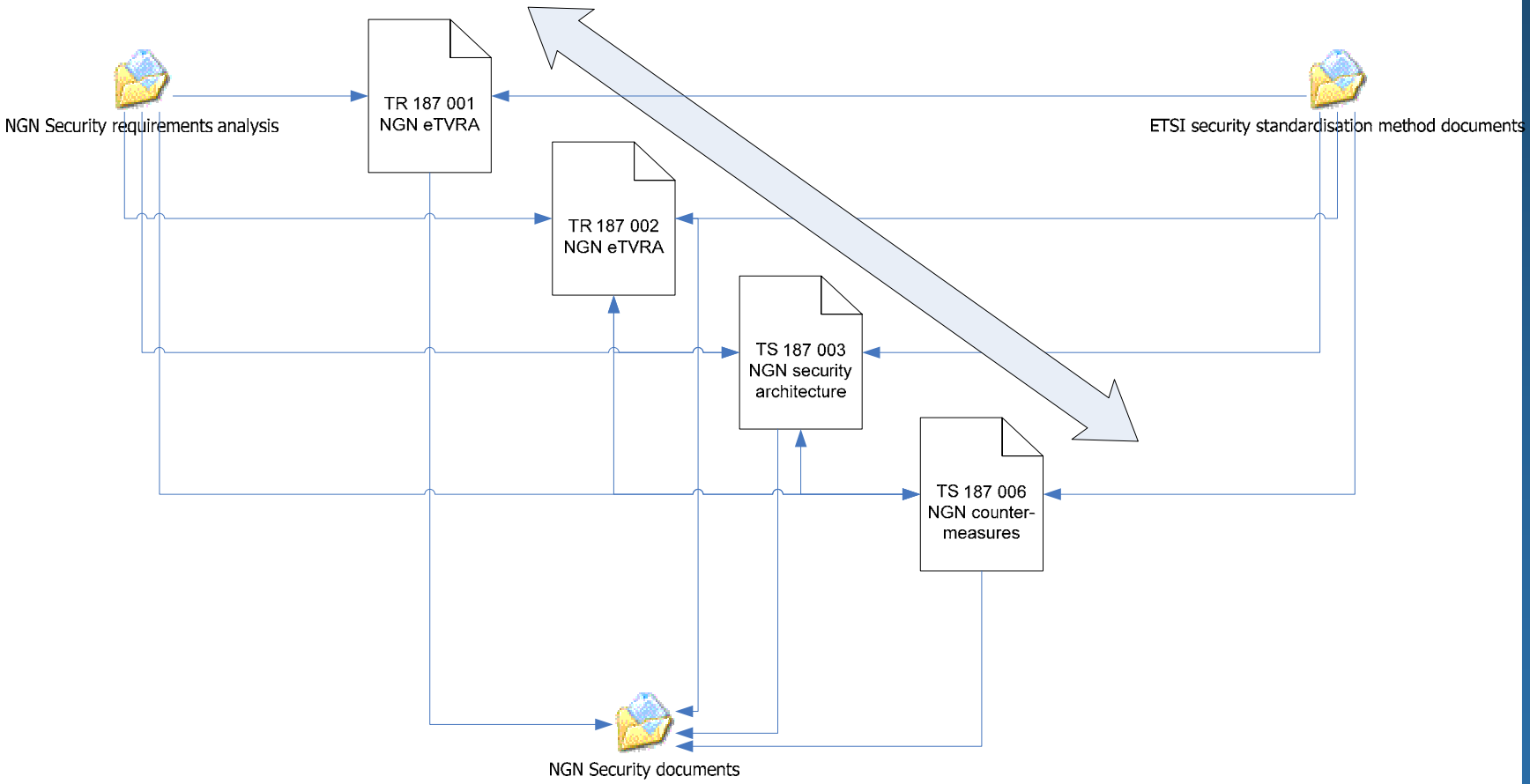
Building up ETSI security frameworks



Requirements engineering and analysis



NGN SEC from common methods



Process for Part 1 (1)

Obtaining security objectives and security requirements:

- Pre-condition: Service Requirements

  - Perform Vulnerability analysis of Service Requirements
  - Identify and specify Security Objectives
  - Refine Security Objectives to Security Requirements
  - Perform GAP analysis to discover any inconsistencies between Security Objectives, Security Requirements and Service Requirements
  - Update Service Requirements and check that these are consistent with security objectives
  - Update Security Objectives and Reqirements