ETSI TR 187 011 V2.1.1 (2008-07)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples

Reference

DTR/TISPAN-07028-NGN-R2

Keywords

security, protocol, methodology

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document defines a method, based on the application of ISO/IEC 15408-2 [i.10], for concisely and unambiguously declaring security requirements expressed in ETSI standards. The purpose of the present document is to provide support to developers of ETSI standards in using the security functional components of ISO/IEC 15408-2 [i.10]. In particular it explains the elements in the ISO/IEC 15408-2 [i.10] 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.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ETSI EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".

[i.2] ETSI ES 202 382: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles".

[i.3] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.4] ETSI TR 102 420: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Review of activity on security".

[i.5] ETSI EG 201 383: "Methods for Testing and Specification (MTS);Use of SDL in ETSI deliverables; Guidelines for facilitating validation and the development of conformance tests".

[i.6] ETSI EG 201 872: "Methods for Testing and Specification (MTS); Methodological approach to the use of object-orientation in the standards making process".

[i.7] ETSI EG 202 106: "Methods for Testing and Specification (MTS); Guidelines for the use of formal SDL as a descriptive tool".

[i.8] ITU-T Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[i.9] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.10] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.11] ISO/IEC 15408-3: "Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements".

[i.12] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".

NOTE: When referring to all parts of ISO/IEC 15408 the reference above is used.

[i.13] Directive 2002/58/EC: "Directive 2002/58/Ec of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic commu-nications sector (Directive on privacy and electronic communications).

[i.14] IETF RFC 4306: "Internet Key Exchange (IKEv2) Protocol".

[i.15] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[i.16] IETF RFC 4305: "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

access service provider: entity that provides the underlying IP transport connectivity between the consumer and the NGN entities

asset: information or resource to be protected by countermeasures

attack interface: point of attack presented by a functional entity that is reachable from outside a trust domain and which exposes the trust domain to one or more forms of malicious action

NOTE: Malicious action may include but not be restricted to denial of service attack, traffic analysis, masquerade, replay attack, penetration and sabotage.

consumer: domain where the IPTV services are consumed

NOTE: The consumer domain may consist of a single terminal, used directly for service consumption, or may be a network of terminals and related devices, including mobile devices. Note that a single consumer domain may be connected obtaining content from multiple Content providers.

content provider: entity that owns or is licensed to sell content or content assets

NOTE: Although the IPTV Service Provider is the primary source for the Consumer, a direct logical information flow may be set up between Content Provider and Consumer, e.g. for rights management and content protection.

IPTV service provider: entity that prepares the content bundle provided by the content provider for delivery to the consumer by providing metadata, content encryption and physical binaries

NGN service provider: entity offering IP based services, which shares a consistent set of policies and common technologies

NOTE: It handles user authentication/identification, Service Control and security, Charging, IPTV common functions, etc. Several IPTV Service Providers could use the same NGN Service Provider to delivery contents to the consumer. The NGN Service Provider may also provide IPTV service.

secure connection: connection between two functional entities that provides properties of confidentiality, authenticity and integrity proof for any transmission across the connection

secure ICT system: physical implementation of a security standard or set of associated security standards

security standard: communications standard that includes provisions for protecting users and networks from threats to the confidentiality and integrity of both identity and data

trust domain: grouping and/or collection of functional entities (implemented in one or more physical devices) whose operation or ownership arrangements mitigate any risk of exploit to the grouping and/or collection within the trust domain boundary

NOTE 1: In the simplest case, a Trust Domain is a set of physical or functional entities with a single owner/operator who can accurately know the behaviour of those physical or functional entities. Such simple Trust Domains may be joined into larger Trust Domains by bi-lateral agreements between the owners/operators of the physical or functional entities.

NOTE 2: A node is "trusted" (with respect to a given Trust Domain) if and only if it is a member of that domain.

NOTE 3: A node, A, in the Trust Domain is "trusted by" a node, B, (or "B trusts A") if and only if there is a secure connection between the nodes, AND B has configuration information indicating that A is a member of the Trust Domain. Further it is noted that B may or may not be a member of the Trust Domain, e.g. B may be a UE which trusts a given network intermediary, A (e.g. its home proxy).

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CSP	Communications Service Provider
EAL	Evaluation Assurance Level
ICT	Information and Communications Technology
IKE	Internet Key Exchange Version 2
IPTV	Internet Protocol TeleVision
MSC	Message Sequence Chart
NAT	Network Address Translation
NGN	Next Generation Network
PATS	Publicly Available Telecommunications Service
RACS	Resource Admission Control Subsystem
SDL	Specification and Description Language
SDPF	Service Policy Decision Function
TOE	Target Of Evaluation
TOE	Target Of Evaluation

TSF	TOE Security Functions
TVRA	Threat, Vulnerability and Risk Analysis
UDP	User Datagram Protocol
UML	Unified Modelling Language

4 Standards, assets and systems

Communications standards specify detailed requirements that must be met by implementations of the standard in order to be compliant. Depending on the range and complexity of the specified requirements, such standards might be implemented by whole systems or by individual component parts of the systems. In those cases where implementations are likely to either provide or exist within a secure environment, the standard will specify addition, security-related requirements derived from a thorough Threat, Vulnerability and Risk Analysis (TVRA) as defined in TS 102 165-1 [i.3]. In TVRA terminology, a system component that implements a communications standard is referred to as an "asset" and this term is used with the same meaning throughout the present document.

In summary:

- Standards specify requirements for both communication and security aspects;
- Assets are implementations of one or more security-related standards; and
- Systems comprise one or more assets.

5 Objectives and requirements in security standards

5.1 Overview

One of the keys to successful system design is the ability to show the relationships which exist between objectives, requirements and the system design. Furthermore, when all the assets of the system can be shown to be necessary by directly mapping to the requirements they implement, it may be said that the design is complete.

The distinction between security objectives and security requirements is an important one to make.

An objective is the expression of what a security system should be able to do in very broad terms whereas a requirement is a more detailed specification of how an objective is achieved. Objectives may be considered to be desires rather than mandates. Security requirements are derived from the security objectives and, in order to make this process simpler, requirements can be further subdivided into functional requirements and detailed requirements.

Functional security requirements identify the major functions to be used to realize the security objectives. They are specified at a level which gives an indication of the broad behaviour expected of the asset, generally from the user's perspective. Detailed security requirements, as their name implies, specify a much lower-level of behaviour which would, for example, be measurable at a communications interface. Figure 1 shows how functional requirements can be extracted from existing specifications and from other input and that they are combined to achieve the security objectives of the target system. Each functional requirement is realized by a number of implementation requirements.

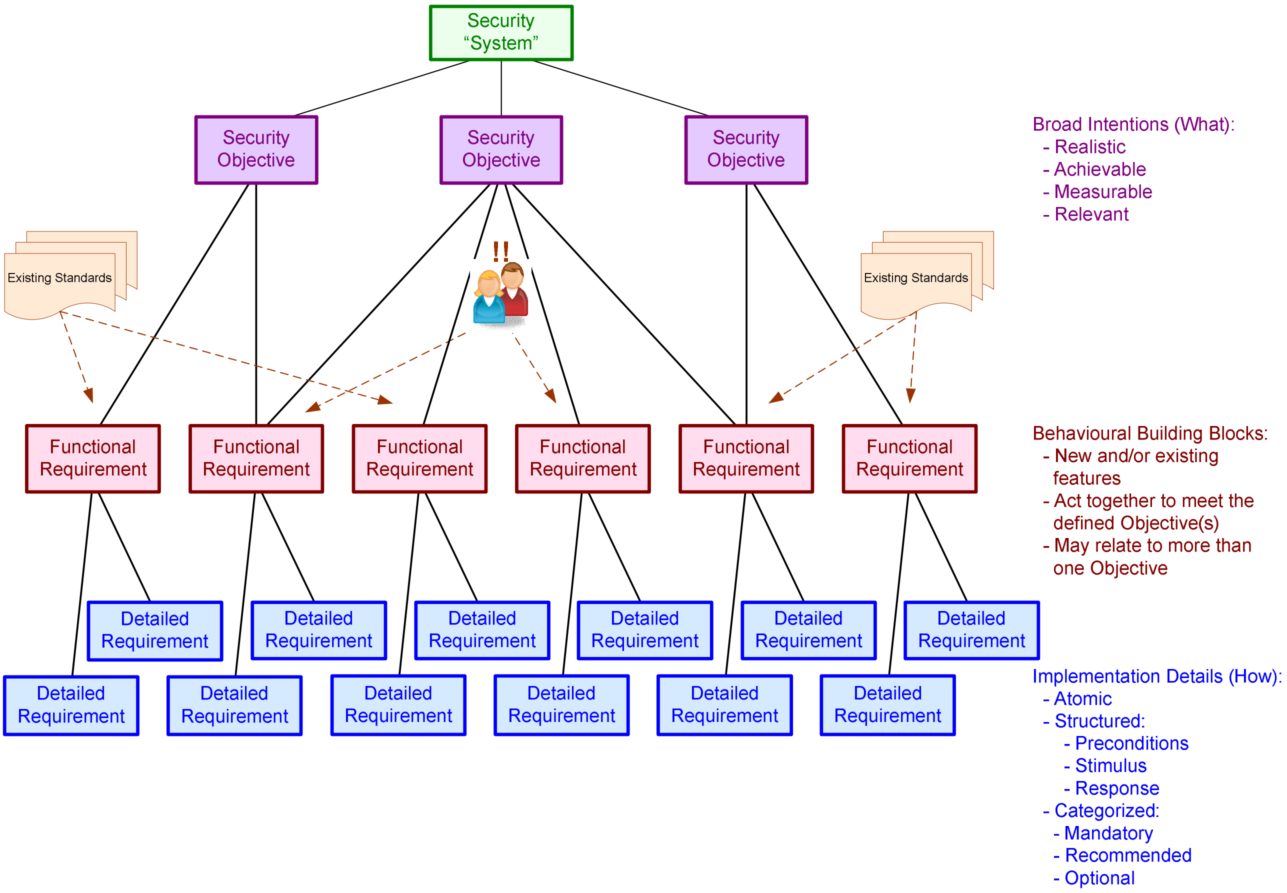

Figure 1: Security objectives and requirements

The following is a simple example of a security objective with a small selection of associated functional requirements and detailed requirements:

- Objective:
  - An NGN should be able to ***restrict access*** to its services so that they are only available to ***validated known users***.
- Functional requirements:
  - An NGN shall allow the establishment of emergency calls on behalf of the user to be performed before the user is identified (from ISO/IEC 15408-2 [i.10] FIA_UID.1.1).
    - This functional requirement arises from asking the question: Is there anything an NGN should allow an unidentified user to do? The answer comes in part from a review of the EU Framework Directive and in particular the Universal Service Directive where some services should be available on a PATS at all times. In addition in some radio networks (e.g. TETRA, GSM) initial camping on a cell is allowed prior to registration and it is registration that involves the exchange of identity.
  - An NGN shall require each user to be successfully identified before allowing any other NGN-mediated actions on behalf of that user (from ISO/IEC 15408-2 [i.10] FIA_UID.1.2).
  - An NGN shall require each user to identify itself before allowing any other NGN-mediated actions on behalf of that user (from ISO/IEC 15408-2 [i.10] FIA_UID.1.1).
- Detailed requirements:
  - An NGN user shall be identified by their NGN CSP assigned identifier in E.164 format.

There are also consequential requirements that need to be taken into account. Whilst in the example a detail requirement is identified this itself requires that the NGN CSP has a means to assign identifiers and to audit the assignment, it will also be necessary to protect the distribution of the identity such that there will be strong assurance that it is given to the correct party.

5.2 Security objectives

The specification of any security system should contain a definition of the security objectives of both the system (including its component assets) and its environment. These objectives are expected to be based upon the assumptions, threats and policies described in the asset security environment. They should be expressed in broad terms rather than in detail and should be segregated into two distinct groups, thus:

- security objectives for the asset:

  A clear definition of which aspects of the identified threats and policies are addressed by each objective;

NOTE 1: If the base security standard specifies a protocol, it is likely that the asset security objectives will be specified in the Stage 1 (or equivalent) specification;

- security objectives for the environment:

  A clear definition of which aspects of the identified threats and policies are expected to be addressed by the environment because they are not covered (either wholly or in part) by the asset security objectives;

NOTE 2: Communications standards rarely specify requirements for the environment so it is unlikely that the security objectives for the environment will be stated explicitly in the base security standard or any associated document.

When developing the security objectives related to a standard it is essential to ensure that each objective is:

- realistic;
- achievable;
- measurable;
- relevant.

NOTE 3: These criteria are a refinement of the commonly used SMART criteria used in some system analysis environments.

Clause 7 provides further details on the meaning of these characteristics.

5.3 Security requirements

5.3.1 Functional security requirements

Security functional requirements should be defined using the model specified in ISO/IEC 15408-2 [i.10] and should be specified for both the asset and, where applicable, its environment. The asset security functional requirements should be classified into the following groups:

- asset security functional requirements:
  - an identification the security functional requirements as specified by reference to the functional components defined in ISO/IEC 15408-2 [i.10] where the assignments and/or selections required have been made for the system under evaluation;

- asset security assurance requirements:
    - An indication of the Evaluation Assurance Level (EAL) as described in ISO/IEC 15408-1 [i.9] that an implementation of the base security standard could be expected to meet. As there are likely to be many implementations in a number of different application areas, the EAL requirement could be expressed as a range (e.g. EAL3 - EAL5);
    - Where possible, an identification of any specific assurance components from ISO/IEC 15408-3 [i.11] which will apply to an implementation; and
    - Where necessary, a specification of any essential assurance requirements which are not included in ISO/IEC 15408-3 [i.11].

5.3.2 Detailed security requirements

Security requirements should be identified for both the asset and, where applicable, its environment. The asset security requirements should be classified into the following groups:

- asset security functional requirements:
    - an identification of each of the security-related functional requirements specified in the base security standard and an indication of where in the standard the detailed requirement can be found;
    - a mapping to the functional security requirement.
- asset security assurance requirements:
    - an indication of the Evaluation Assurance Level (EAL) as described in ISO/IEC 15408-1 [i.9] that an implementation of the base security standard could be expected to meet. As there are likely to be many implementations in a number of different application areas, the EAL requirement could be expressed as a range (e.g. EAL3 - EAL5);
    - where possible, an identification of any specific assurance components from ISO/IEC 15408-3 [i.11] which will apply to an implementation;
    - where necessary, a specification of any essential assurance requirements which are not included in ISO/IEC 15408-3 [i.11].

The specification of security requirements for the environment is optional and should only be included in the analysis if security objectives for the environment are identified earlier in the analysis (see clause 5.2). If requirements for the environment are included, they should be presented in the same way as functional requirements for the asset.

6 Threat Analysis

Although many of the security objectives and requirements related to a particular target system or asset will be self-evident, a full Threat, Vulnerability and Risk Analysis (TVRA) [i.3] is an essential activity in ensuring that all objectives and requirements are identified and specified. Both TVRA and the specification of security objectives and requirements should be integrated into the normal standards engineering process. As shown in figure 2, the process is iterative with the possibility that series of activities can be repeated until the specification of operational and security requirements is complete. Even with the addition of activities related to the specification of security objectives and requirements, this process still maps well to the 3-stage process defined in ITU-T Recommendation I.130 [i.8].

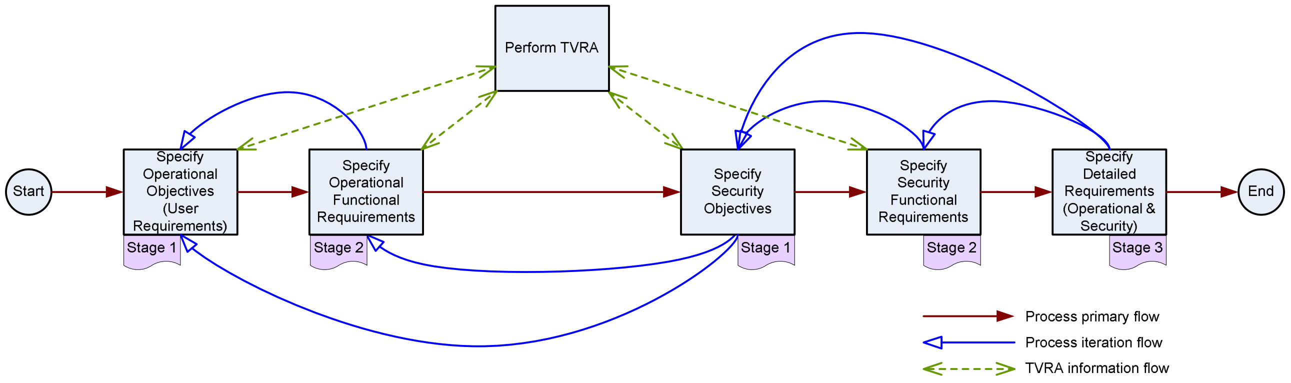
Perform TVRA
Start
Specify Operational Objectives (User Requirements)
Stage 1
Specify Operational Functional Requuirements
Stage 2
Specify Security Objectives
Stage 1
Specify Security Functional Requirements
Stage 2
Specify Detailed Requirements (Operational & Security)
Stage 3
End
Process primary flow
Process iteration flow
TVRA information flow

Figure 2: Standards development process including security aspects

TVRA should be performed at various stages throughout the process. A basic analysis should be carried out as soon as the initial operational objectives have been specified. A more detailed threat analysis should then be undertaken when the operational user requirements (stage-1) and functional requirements (stage-2) have been defined. These analyses should result in the specification of the security objectives. A further TVRA should be performed at this stage in order to determine whether these security objectives do, in fact, counter all of the identified threats without creating additional vulnerabilities.

7 Specifying security objectives

7.1 Getting started

Before attempting to identify the security objectives of a system and its environment, it is first necessary to understand the operational objectives of the system and the nature of the environment in which it is expected to exist. For example, knowledge that one the operational objectives of a system is "*to provide simple telephony between two or more public internet subscribers*", makes it possible to consider what its fundamental security objectives should be.

At this early stage it is essential that the boundary between the system (the target of standardization) and its environment is defined. Without this definition, it is likely that at least some of the security objectives specified will be impossible to meet. There are no strict rules on how to determine what is in the system and what is in its environment but, as a guide, in communication systems it is likely that the boundary will pass through interfaces rather than entities and that human users will exist within the environment rather than the system. It is also likely that the system will comprise a number of easily identifiable assets which may be decomposed into multiple assets themselves at a later stage in the development process. The simple example in figure 3 shows graphically the boundary between a system and its environment.

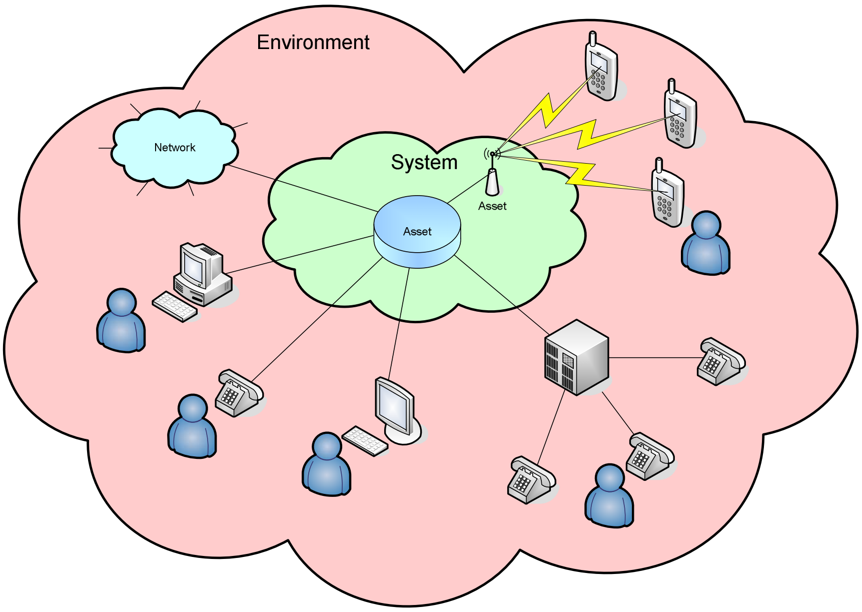

Figure 3: Example of a security system with its environment

7.2 Identifying security objectives

A system's operational requirements specify what it should do. The starting point for its security objectives is to consider what it should not do. In the example above, it would be reasonable to expect that the system should not provide telephony service to unknown or unauthorized users and this might lead to a security objective which specifies that "*the system should limit access to its services to validated known users*".

The identification of security objectives should be based upon a rigorous analysis of threats, vulnerabilities and risks as is defined in TS 102 165-1 [i.3]. Such an analysis should be performed at various stages within the development process to ensure that any changes caused by the addition of operational and security objectives and requirements are evaluated and incorporated into the security model.

Security objectives specified for the system's environment should be limited to those assumptions which have a direct or indirect impact on the behaviour of the system itself. For example, it would be unreasonable to state that "*the environment should limit access to its services to validated known users*". However, it would be reasonable to specify that "*the environment should comply with EU Directive 2002/58/EC (and its amendments) on Privacy*" [i.13].

Within the context of communications standards, security objectives, whether for the system or the environment, should never prescribe the behaviour of human users (which cannot be controlled or predicted). Any objective which does so should be reviewed and either revised to make it impersonal or removed altogether.

7.3 Formulating security objectives

Security objectives should reflect the high-level goals of the system in providing an appropriate secure environment for users of the system. This means that they should be expressed:

- in terms of the expected behaviour of an implementation of the target standard(s). For example:
  - an implementation of ES 234 567;
  - an IPv6 router;
  - an IMS CSCF;
- as desires rather than strict requirements:
  - use "should" rather then "shall";

- as abstract, system-wide capabilities. For example:
  - an IPsec host should be able to ensure that data transmitted to another IPsec device cannot be revealed to a third (unwanted) party.

Furthermore as defined in TS 102 165-1 [i.3] security objectives should fall into a small set of classes relating to core security attributes:

- confidentiality;
- integrity;
- authenticity;
- availability.

7.4 Validating security objectives

As a first step, all security objectives should be assessed to ensure that they meet the following criteria (see clause 5.2) of being:

- realistic:
  - The objective does not make unjustifiable demands on the target system. For example, in a secure environment it would be unrealistic to set an objective that all users should be able to view the secret passwords of all other users;
- achievable:
  - it should be possible to meet the objective within the bounds of current or emerging technology without unreasonable cost;
- measurable:
  - Once an objective has been met, it should be possible to view or otherwise validate its effect on the target system either directly or indirectly;
- relevant:
  - the objective should be directly related to the general security of the target system and its environment;
  - The objective should not detract from the overall purpose of the target system.

If a security objective is unable to meet all of these criteria, it should be revised or rejected.

A further TVRA should then be carried out to determine whether the specified security objectives would, if implemented, provide adequate countermeasures to the perceived threats to the system.

As part of the validation process, all security objectives should be reviewed with potential implementers and users of the associated standards.

In order to prove that security has been addressed there is often a requirement to maintain logs (audit records) of actions that will be used to address the requirement to be measurable.

8 Requirements capture

8.1 The characteristics of requirements

Having established the security objectives related to a communications standard, it is necessary to identify the specific security requirements which, when implemented, will achieve the objectives. In order to simplify this process, security requirements are segregated into two distinct types (as described in clause 5.3) which are specified at different levels of detail, as follows:

- functional requirements:
  - high-level requirements;
  - behavioural building blocks;

NOTE: A building block may be a top level function such as "Authentication" or "Key Management" but may be more detailed if required.

  - may refer to existing protocol and service standards;
  - should be expressed in terms of the capabilities specified in ISO/IEC 15408-2 [i.10].
- detailed requirements:
  - low-level requirements;
  - expressed in a structured form:
    - preconditions;
    - stimulus;
    - response;
  - may be a simple reference to an existing standard.

8.2 Specifying requirements

8.2.1 Functional requirements

There is no simple or automatic method for extracting functional requirements from a security objective. In most cases it is a matter of asking questions such as "*How can this objective be achieved?*" or "*What behaviour is necessary to achieve this objective?*". As an example, if an objective states that "*An implementation should be able to ensure that data transmitted to another implementation cannot be revealed to a third (unwanted) party during transmission*" then an analysis of this statement identifies a requirement to protect user data (the data being transmitted) from eavesdropping (a threat). The functional building block from ISO/IEC 15408-2 [i.10] needed to achieve the example objective can be found in the User Data Protection class, as follows:

- The implementation shall enforce policies to be able to transmit data in a manner protected from unauthorized disclosure (FDP_UCT.1.1).

Alternatively the objective can be considered in the context of existing external specifications using the following example functional requirements:

- an implementation of this standard shall also implement the Internet Key Exchange protocol, IKEv2, as specified in RFC 4306 [i.14];
- an implementation of this standard shall also implement the IP Encapsulating Security Payload (ESP) as specified in RFC 4303 [i.15] and RFC 4305 [i.16].

In this particular case, the detailed requirements are already specified in RFCs 4303, 4305 and 4306 and do not need to be specified further unless specific profiles of these specifications are required. Functional requirements might equally be expressed without reference to existing specifications. Such requirements would then need to be decomposed into a number of detailed requirements.

The specification of functional requirements should be limited to the following:

- only those requirements that contribute to the achievement of the security objectives;
    - if a new functional requirement is adjudged to specify essential security behaviour but cannot be shown to contribute to the achievement of any of the security objectives, a further TVRA should be undertaken in order to identify any additional objective(s).
- only those requirements that are likely to have an impact on the communications services and/or protocols of an implementation of the target standard(s).

A functional security requirement should be expressed in a form that indicates whether the requirement is:

- mandatory: uses the verb "shall"

EXAMPLE 1: "*An implementation shall authenticate a user by means of a username and password*".

- recommended: uses the verb "should"

EXAMPLE 2: "*An implementation should ensure that a user provides a valid identification prior to the start of a communications session*".

- optional: uses the verb "may"

EXAMPLE 3: "*An implementation may use the NULL encryption algorithm to provide authentication and integrity if confidentiality is not a necessity*".

8.2.2 Detailed requirements

Detailed security requirements specify the individual elements of service or protocol behaviour that a system must implement if it is to fully achieve the associated security objectives. In many cases, the functional requirements will identify that detailed requirements can be derived directly from existing standards and international specifications (see the examples in clause 8.2.1). However, if no such specification exist, it may be necessary to define completely new security requirements.

The development of detailed security requirements should begin with a review of the functional security requirements to determine how each of these can be broken down into lower level elements of behaviour. The use of graphical techniques such as SDL process charts, MSCs or UML activity diagrams can be very effective in identifying the detailed requirements which are the components of functional requirements. Useful guidance on this process can be found in EG 201 383 [i.5], EG 201 872 [i.6] and EG 202 106 [i.7] as well as the ETSI "Making Better Standards" web site (http://portal.etsi.org/mbs).

The process of decomposing functional security requirements should ensure that the resultant detailed requirements are atomic in that they specify single elements of service or protocol behaviour. Each detailed requirement should consist of the following:

- An optional precondition which indicates the circumstances or context that must be established before the requirement becomes valid.

EXAMPLE 1: "If an IKEv2 implementation supports NAT traversal, …."

- A stimulus defining the action which causes the security system to initiate a visible (measurable) response.

EXAMPLE 2: "…an IKEv2 implementation receives a IKE message on UDP port 500…"

- A response defining the behaviour of the implementation on receiving the defined stimulus.

EXAMPLE 3: "...the IKEv2 implementation must set the Destination Port Number to 500 in the UDP header of the response message."

There is no strict rule governing the order in which the precondition, stimulus and response should appear in an individual requirement. They should be arranged in such a way that the overall requirement is unambiguous and easy to read. The examples above could, therefore, be combined into a single detailed security requirement, thus:

> *"If an IKEv2 implementation that supports NAT traversal receives an IKE message on UDP port 500, it must set the Destination Port Number field to 500 in any message sent in response."*

The guidelines specified in clause 8.2.1 regarding functional security requirement types (mandatory, recommended or optional) apply equally to detailed security requirements.

9 Specifying security objectives and requirements using ISO/IEC 15408-2

9.1 Overview

ISO/IEC 15408-2 [i.10] specifies a formal set of functional requirements (components) which together describe the security behaviour expected of a secure ICT system. Each functional component comprises one or more indivisible elements in which the requirement text is define. The documentation used for the evaluation of the security capabilities of such a system is required to identify security functionality from the range of components defined in ISO/IEC 15408-2 [i.10].

ISO/IEC 15408 [i.12] refers to a secure ICT system as a Target Of Evaluation (TOE). Within the standards development environment, a TOE should be considered to represent a "system under standardization". Similarly, the term TOE Security Function (TSF) refers to each of those functions within a system which will provide security to the users of the system.

9.1.1 The structure of functional components

ISO/IEC 15408-2 [i.10] groups related functional components into families which are then grouped further into "classes" as shown in figure 4.

NOTE: These classes should not be confused with the same term commonly used in Object Oriented Design and Analysis.

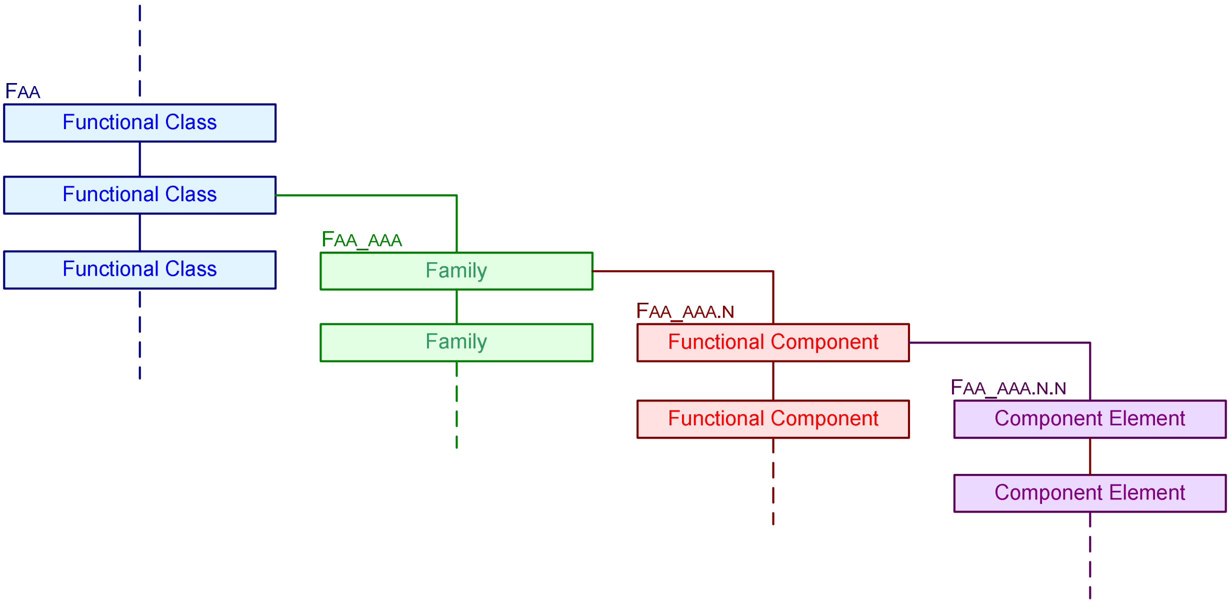

Figure 4: Hierarchical structure of functional components

ISO/IEC 15408-2 [i.10] uses a structured identification system for classes, families components and elements as follows:

- each functional class is given a unique 3-letter identifier which starts with the letter "F";
- family identifiers are constructed from the appropriate class identifier followed by another unique 3-letter mnemonic;
- component identifier consists of the family identifier followed by a one or two digit number;
- elements of each component are identified using a one or two digit number appended to the associated component id.

The clear and complete structure of functions described in ISO/IEC 15408-2 [i.10] makes it a useful tool in the derivation of security objectives and requirements. By considering each functional class, it is likely that full range of objectives can be determined. It is not certain that all the functional classes will be included in the objectives but at least all of them will have been considered. Families and, to some extent, components can be used in the same way to identify functional requirements while components and their elements will help in the determination of more detailed requirements.

A well formed statement of an objective should contain a number of key words that will indicate the class of functional capabilities likely to assist in getting to a detail requirement. The following example is a clear and concise objective.

EXAMPLE: An NGN should be able to ***restrict access*** to its services so that they are only available to ***validated known users***.

This statement identifies both the TOE and the outline of the TSFs expected in general terms. The TOE in the example is an NGN which is the entity with responsibility for the security and other functions. The set of TSFs are those dealing with access restriction and with identifying and validating users. The use of the term validation implies authentication.

9.1.2 ISO/IEC 15408-2 functional classes

EG 202 387 [i.1] describes how the ISO IEC 15408-2 [i.10] functional classes, families and components can be interpreted in the context of standards development. Table 1 lists each of the functional classes and their associated families. A detail analysis of the full range of functional components from ISO/IEC 15408-2 [i.10] is listed in TR 102 420 [i.4].

Table 1: ISO/IEC 15408-2 functional classes and families

Functional class	Class ID	Family	Family ID
Security audit	FAU	Security audit automatic response Security audit data generation Security audit analysis Security audit review Security audit event selection Security audit event storage	FAU_ARP FAU_GEN FAU_SAA FAU_SAR FAU_SEL FAU_STG
Communication	FCO	Non-repudiation of origin Non-repudiation of receipt	FCO_NRO FCO_NRR
Cryptographic support	FCS	Cryptographic key management Cryptographic operation	FCS_CKM FCS_COP
User Data Protection	FDP	Access control policy Access control functions Data authentication Export to outside TSF control Information flow control policy Information flow control functions Import from outside of the TOE control Internal TOE transfer Residual information protection Rollback Stored data integrity Inter-TSF user data confidentiality transfer protection Inter-TSF user data integrity transfer protection	FDP_ACC FDP_ACF FDP_DAU FDP_ETC FDP_IFC FDP_IFF FDP_ITC FDP_ITT FDP_RIP FDP_ROL FDP_SDI FDP_UCT FDP_UIT

Functional class	Class ID	Family	Family ID
Identification and authentication	FIA	Authentication failures User attribute definition Specification of secrets User authentication User identification User-subject binding	FIA_AFL FIA_ATD FIA_SOS FIA_UAU FIA_UID FIA_USB
Security management	FMT	Management of functions in TSF Management of security attributes Management of TSF data Revocation Security attribute expiration Specification of management functions Security management roles	FMT_MOF FMT_MSA FMT_MTD FMT_REV FMT_SAE FMT_SMF FMT_SMR
Privacy	FPR	Anonymity Pseudonymity Unlinkability Unobservability	FPR_ANO FPR_PSE FPR_UNL FPR_UNO
Protection of the TSF	FPT	Underlying abstract machine test Fail secure Availability of exported TSF data Confidentiality of exported TSF data Integrity of exported TSF data Internal TOE TSF data transfer TSF physical protection Trusted recovery Replay detection State synchrony protocol Time stamps Inter-TSF TSF data consistency Internal TOE TSF data replication consistency TSF self test	FPT_AMT FPT_FLS FPT_ITA FPT_ITC FPT_ITI FPT_ITT FPT_PHP FPT_RCV FPT_RPL FPT_SSP FPT_STM FPT_TDC FPT_TRC FPT_TST
Resource Utilization (FRU)		Fault tolerance Priority of service Resource allocation	FRU_FLT FRU_PRS FRU_RSA
TOE Access	FTA	Limitation on scope of selectable attributes Limitation on multiple concurrent sessions Session locking TOE access banners TOE access history TOE session establishment	FTA_LSA FTA_MCS FTA_SSL FTA_TAB FTA_TAH FTA_TSE
Trusted path/channels	FTP	Inter-TSF trusted channel Trusted path	FTP_ITC FTP_TRP

9.2 Characterizing functional components

The ISO/IEC 15408-2 functional components are specified in a generic form that could apply to any ICT system. However, many of these components can be characterized for specific application areas by expanding the [**selection**:….] and [**assignment**:….] tags that are included in the text of many of the component elements for this exact purpose. As an example, the functional element FAU_STG.2.3 (Security audit event storage : Guarantees of audit data availability) specifies the following:

> *The TSF shall ensure that [**assignment**: metric for saving audit records] audit records will be maintained when the following conditions occur: [**selection**: audit storage exhaustion, failure, attack].*

This could be expressed as a requirement in a security standard related to the operation of an NGN Security Gateway as follows:

> *An NGN Security Gateway shall ensure that at least 200 audit records are maintained for each established Security Association when any of the following conditions occur:*
>
> - *audit record memory overflow;*
> - *gateway system failure;*

- *network failure; or*
- *the detection of a malicious attack on the gateway.*

As can be seen from the example above, limited adaptation of the base text is permitted but it is necessary that the resultant text is recognizable as having been derived from the specific component element.

9.3 Identifying ISO/IEC 15408-2 component elements in standards

Although ISO/IEC 15408-2 [i.10] requires the specification of a secure ICT system to positively identify each component element used within the specification, it is not necessary for this information to be included directly within a security standard. In order to maintain the readability and "flow" of a standard, a companion document, the Protection Profile as defined in ES 202 382 [i.2], should be produced to summarize the security objectives that the standard(s) claim to meet and the security requirements expressed within the standard(s). Both the objectives and the requirements are cross-referenced to specific clauses in the standard(s). The Protection Profile extract shown in figure 5 summarizes the requirement shown in clause 9.2.o-è

c IT Security Requirements c.1 TOE security requirements			
c.1.1TOE security functional requirements			
..	..	..	..
c.1.7.5	Maintenance of stored audit records	FAU.STG.2.3	ES 321 123 clause 4.1.2
..	..	..	..

Figure 5: Example extract from a Protection Profile

9.4 Integration with TVRA

The role of TVRA [i.3] in the development of Protection Profiles is in establishing the rationale for the security features in the Protection Profile [i.2].

Annex A: Worked examples of using the method in NGN applications

A.1 RACS

As an example, a single objective from RACS in NGN R2 is developed through functional requirement to detailed requirements with a view to refining the objective such that it meets the requirements outlined in the method in the present document.

The initial objective statement is as follows:

> *The NGN R2 RACS should have means to ensure confidentiality of sensitive information on resource reservations stored on SPDF and x-RACF.*

A simple analysis of this statement identifies the Target of Evaluation (TOE) as the NGN RACS (in particular for NGN Release 2), and the key capability is the confidentiality of stored information. In this case the SDPF and the x-RACF sub-elements (assets) of the TOE are defined as targets. This suggests that the objective should possibly be split into two separate objectives as follows:

> *The NGN R2 RACS should have means to ensure confidentiality of resource reservation data stored on SPDF.*

> *The NGN R2 RACS should have means to ensure confidentiality of resource reservation data stored on x-RACF.*

In each case the security function is clearly identified as *confidentiality* and the entity that it addresses is identified as *stored resource reservation data*. The next step is to identify the relevant functional classes from ISO/IEC 15408-2 [i.10].

Once more in the modified objectives are important in the analysis as they refer to both confidentiality and to stored data. In trying to identify a single functional class from ISO/IEC 15408-2 [i.10] some of the difficulty in using the common criteria as a development guide rather than an evaluation tool becomes apparent. A first glance may suggest that the functional requirement comes from the "User Data Protection" class (Stored data integrity or Inter-TSF user data confidentiality transfer protection), or even from the "Protection of the TSF" class (confidentiality of exported data). However this simple analysis suggests an invalid objective because what appears to be required is that the stored data is accessible only to appropriately authorized entities. This, then, requires that the objective is rewritten as follows:

> *The NGN R2 RACS should have means to ensure that access to stored resource reservation data on the SPDF is only provided to authorized entities.*

This then provides a map to the "User Data Protection" class and to the families within that class of "Access control policy" and "Access control functions". In addition, the objective and its dependent functional requirements will then include a means to identify and verify the accessing entity.

In the original objective statement the keyword *sensitive* was present. Further analysis of this has not been undertaken as sensitive is not a security keyword by itself. The sensitivity of any data element depends on its use when compromised. In the detailed design stage (not illustrated here) the designer will need to determine how access control should be applied to each data element in the resource reservation set.

A.2 Unsolicited communication

The example given here is of a single objective for the prevention of unsolicited communication in NGN R2 and its expansion through functional requirement to candidate detail requirements with a view to refining the objective such that it meets the requirements outlined in the method in the main body of the present document.

The objective statement is as follows: *The NGN should provide the ability to a user to personalize his UC profile.*

The TOE for this objective is the NGN and the objective requires an identified person to manage data. The first refinement is to change the word ability to means as this makes a stronger link to methods or functions that are to be provided by the NGN standards. The mildly refined objective then reads: *The NGN operator should provide means for a user to personalize his UC profile.* The functional classes from ISO/IEC 15408-2 [i.10] required are **Identification and authentication** and **User data protection**.

A.3 Media security

The example given here is of a single objective for media security in NGN R2 and its expansion through functional requirement to candidate detail requirements with a view to refining the objective such that it meets the requirements outlined in the method in the main body of the present document.

The objective statement is as follows: *An NGN should provide mechanisms to prevent eavesdropping of traffic*.

The major concern expressed here is indicative of the change from PTSN to NGN. In the PSTN security provisions were mostly physical as the access to the line in order to eavesdrop on traffic, or to inject and modify signalling, was presumed difficult, furthermore as the terminal devices were dumb (i.e. did not make any processing decisions) it was straightforward to partition trusted and untrusted areas of the network. In the NGN the assumptions have changed. It is assumed in the NGN that eavesdropping of traffic is possible, and that as terminal devices have intelligence (i.e. processing power and state manipulation capability) that injection and modification of signalling is possible by manipulation at the end-points.

In the general case an attacker might be located along the media path; the signalling path; or, both the media and the signalling path. If the simplest case of end-user traffic is located only on the signalling path then media security, and the objective to provide mechanisms to prevent eavesdropping, may be by examination of the media path only. Examination of the objective statement suggests *mechanisms to prevent eavesdropping* whereas it may be more correct to state that: *An NGN should provide mechanisms to prevent exploit of traffic from eavesdropping.* The rationale is that by moving the objective through the analysis of criteria that objectives have to meet it is required to ask if it is reasonable to be able to detect eavesdropping and in many cases this is clearly unreasonable. For example if the media path is via radio it is possible to eavesdrop without detection and restriction of a radio interface such that it is not possible to eavesdrop is similarly unreasonable.

Further analysis of the objective requires that the media path is itself specified and this requires mapping to elements in the NGN architecture. If it is assumed that the media consumer is outside the NGN and that the media source is within the NGN the functional class **Protection of the TSF** and the family **Confidentiality of exported TSF data** apply. The means to provide confidentiality of data is generally enabled by encryption and the specific means of encryption used is often media dependent. This requires mapping from the objective statement to the **Cryptographic support** class for both the **Cryptographic key management** and **Cryptographic operation** families. The requirement to specify the end points of the protected media path is also inherent in the use of encryption as it these end points that will be involved in the keying operations.

A.4 IPTV

The example given here is of a single objective for the security of IPTV provision in NGN R2 and its expansion through functional requirement to candidate detail requirements with a view to refining the objective such that it meets the requirements outlined in the method in the main body of the present document.

The objective statement is as follows: *An NGN R2 IPTV shall allow for proper accountability of consumers usage of IPTV services for billing purposes.*

The initial keyword analysis of this statement identifies NGN IPTV as the TOE and the core service as accounting for use as part of a billing system. The keyword *proper* is invalid and as an objective the use of the word *shall* is misleading as an objective is a statement of intent and not a mandate (although it should lead to mandates). This leads to the first revision of the objective as: *An NGN R2 IPTV service should provide means to ensure that billing services have access to usage records for the IPTV service*. In order to achieve this the service should identify billing points and billing identities. It has to be determined by the service if it can be accessed only by identified parties, and if such parties need to be authenticated. From this analysis the objective may be either further refined or rejected as it fails to satisfy the analysis criteria for objectives.

History

Document history		
V2.1.1	July 2008	Publication