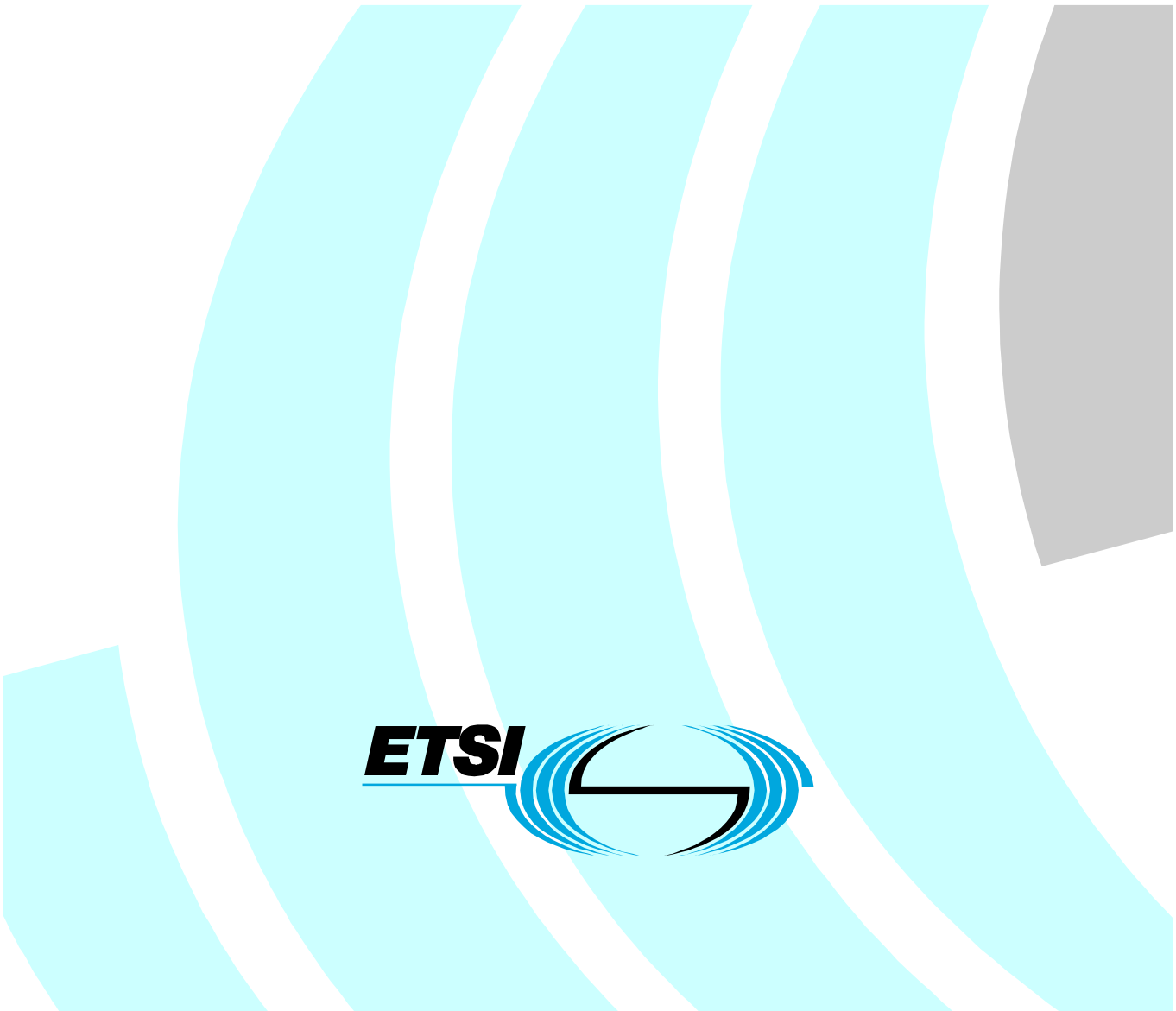
ETSI TS 102 556 V1.1.1 (2006-11)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protection Profile



Reference
DTS/TISPAN-07008-Tech

Keywords
H.248, IMS, internet, profile, protection, security

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

Introduction

The present document is one of a set of documents that addresses standardization of security protocols and mechanisms within the context of the *e*Europe 2005 programme. The documents in this suite are composed as follows:

- ETSI EG 202 387 [4]: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".
- ETSI ES 202 383 [5]: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Security Targets".
- ETSI ES 202 382 [6]: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles".
- ETSI TS 102 165-1 [1]: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Method and proforma for Threat, Risk, Vulnerability Analysis".
- ETSI TS 102 165-2 [2]: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protocol Framework Definition; Security Counter Measures".
- **The present document ETSI EN 102 556: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protection file".**
- ETSI EG 287 www: "Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN); Design Guide; Application of security countermeasures to service capabilities".

These documents are developed based on the objectives of the *e*Europe programme and are also developed to ensure they comply with the overall objectives of the European regulatory framework as defined in the following documents:

- Directive 2002/19/EC of the European Parliament and of the council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive).
- Directive 2002/20/EC of the European Parliament and of the council of 7 March 2002 on the authorization of electronic communications networks and services (Authorization Directive).
- Directive 2002/21/EC of the European Parliament and of the council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).
- Directive 2002/22/EC of the European Parliament and of the council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).

- 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 communications sector (Directive on privacy and electronic communications).

In particular the present document forms part of the standardization initiative for the Next Generation Network (NGN) platform to be used in *e*Europe and upon which the trust and viability of the *e*-enabled community will, to a very large part, depend.

The *e*Europe 2005 action plan has been drawn up to focus on "*the widespread availability and use of broadband networks throughout the Union … and the security of networks and information, eGovernment, eHealth and eBusiness*" requiring a supporting infrastructure, which is truly pan-European. To quote COM(2002)263: "*By 2005 Europe should have … a secure information infrastructure*".

1 Scope

The present document defines 3 partial Protection Profiles (PPs) for security capabilities in the NGN and conforms to the guidance and PP Proforma available in ES 202 382 [6] with respect to the guidelines found in EG 202 387 [4]. The background and input for the PPs are presented in clause 4. The PPs are detailed in annexes to the present document as follows:

- Annex A: PP for NGN-IMS authentication, source document TS 133 203 [9].
- Annex B: PP for NGN-NDS source authentication, source document TS 133 210 [10].
- Annex C: PP for NGN H.248 deployment, source document ES 283 002 [8].

The present document is for the use of NGN standards developers and may be used in the context of formal evaluation.

NOTE 1: A PP is one of the document types subject to evaluation under the evaluation criteria defined in ISO/IEC 15408 [11]. The evaluation criteria are commonly known as the Common Criteria (CC) and in the present document "Common Criteria" is used synonymously to ISO/IEC 15408 [11] (and its Part 1-3 derivatives).

NOTE 2: The present document has not been submitted by ETSI for formal evaluation. Its intended use is to be a basis for future PPs in the area.

The context of the present document is depicted in figure 1.

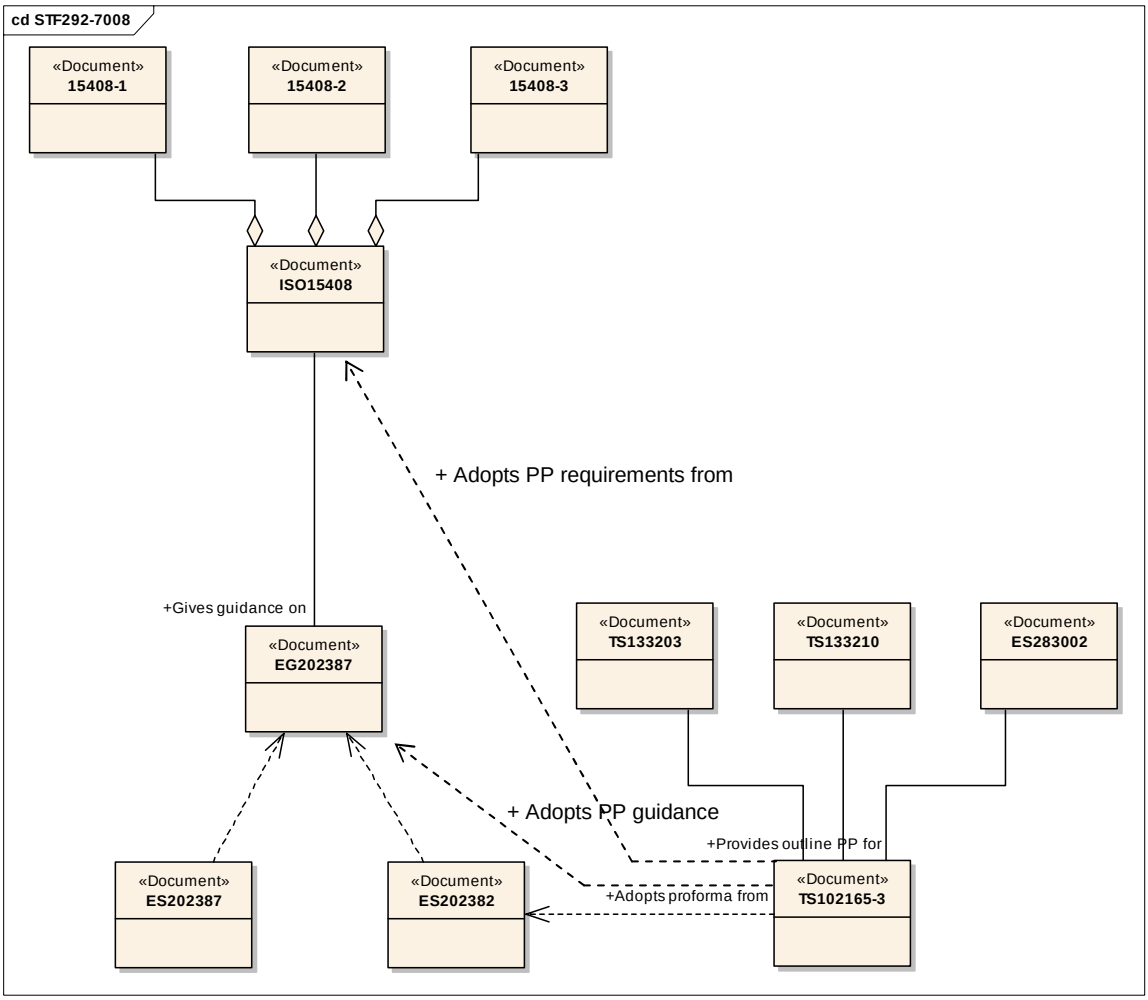


Figure 1: Context of the present document, with main source documents

The PPs in the present document may be primarily considered as measures of completeness of the standardization effort. A security standard is considered complete and suitable for evaluation when every part of the proforma can be filled in by reference to the standardization process and the output documents from that process. Thus it can be conveyed to an assessor that the security development process and the steps towards assurance have been dealt with properly.

The purpose of the PPs in the present document is to assist manufacturers by having agreed content that may be used by them in the process of having a product evaluated using the Common Criteria concept. The PPs may be used as part of the manufacturer's documentation suite for use in an evaluation of a product.

The intention of ETSI is not to have the presented PPs evaluated and certified in ETSI's name. The PPs in the present document are not complete enough for submission for evaluation, but provides the basis to be added to (worked on) for use in group development. Thus the annexes show generic outlines of PPs open for further refinement.

Each PP is open for extended functionality as described in the Common Criteria ISO/IEC 15408-3 [14].

NOTE 1: Extension, according to the Common Criteria ISO/IEC 15408-3 [14], of any of these PPs is open for future work, and should be performed to improve the commercial usability.

NOTE 2: The present Protection Profiles are provided as examples only. They are not intended to be registered or stored by ETSI in any archive or registry in any Common Criteria context.

The PP format used in the present document complies with the proforma in annex A of ES 202 382 [6].

NOTE 3: Relevant requirements from other sources than the target document and the guidance documents have been included in the requirement section.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- 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.
- For a non-specific reference, the latest version applies.

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

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

[1] ETSI TS 102 165-1 (V4.1.1): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis".

[2] ETSI TS 102 165-2 (V4.1.1): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 2: Counter Measures".

[3] ETSI TS 187 001 (V1.1.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[4] ETSI EG 202 387 (V1.1.1) : "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".

[5] ETSI ES 202 383 (V1.1.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Security Targets".

[6] ETSI ES 202 382 (V1.1.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles".

[7] ETSI ES 282 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); Functional architecture".

[8] ETSI ES 283 002 (V1.1.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Subsystem (PES); NGN Release 1 H.248 Profile for controlling Access and Residential Gateways".

[9] ETSI TS 133 203 (V7.0.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services (3GPP TS 33.203 version 7.0.0 Release 7)".

[10] ETSI TS 133 210 (V7.0.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G Security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 version 7.0.0 Release 7)".

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

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

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

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

[15] IETF RFC 1750: "Randomness Recommendations for Security".

[16] IETF RFC 2401: "Security Architecture for the Internet Protocol".

[17] IETF RFC 2407: "The Internet IP Security Domain of Interpretation for ISAKMP".

[18] IETF RFC 2408: "Internet Security Association and Key Management Protocol (ISAKMP)".

[19] IETF RFC 2409: "The Internet Key Exchange (IKE)".

NOTE: RFC 2409 has been superseded by RFC 4306.

3 Definitions and abbreviations

3.1 Definitions

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

access control: See definition in TS 102 165-2 [2].

assets: information or resources to be protected by the countermeasures of a TOE (ISO/IEC 15408-1 [12])

assurance: grounds for confidence that an entity meets its security objectives (ISO/IEC 15408-1 [12])

authentication: provision of assurance of the claimed identity (TS 102 165-2 [2]).

NOTE: (1) Challenge response based authentication; (2) Message authentication code based authentication.

authentication data: information used to verify the claimed identity of a user (ISO/IEC 15408-1 [12])

authorized user: user who may, in accordance with the TSP, perform an operation (ISO/IEC 15408-1 [12])

challenge response based authentication: See definition in TS 102 165-2 [2].

Common Criteria (CC): Used to denote standard ISO/IEC 15408 [11], with Part 1 (ISO/IEC 15408-1 [12]), Part 2 (ISO/IEC 15408-2 [13]) and Part 3 (ISO/IEC 15408-3 [14]).

complete: all necessary parts of an entity have been provided

NOTE: In terms of documentation, this means that all relevant information is covered in the documentation, at such a level of detail that no further explanation is required at that level of abstraction (ISO/IEC 15408-3 [14]). Cf. PP evaluation.

confidentiality: See definition in TS 102 165-2 [2].

consistent: describes a relationship between two or more entities, indicating that there are no apparent contradictions between these entities (ISO/IEC 15408-3 [14])

NOTE: Cf. PP evaluation.

countermeasure: See definition in TS 102 165-2 [2].

evaluation: assessment of a PP, an ST or a TOE, against defined criteria (ISO/IEC 15408-1 [12])

extension: addition to an ST or PP of functional requirements not contained in ISO/IEC 15408-2 [13] and/or assurance requirements not contained in ISO/IEC 15408-3 [14]

IM Subscriber Identity Module (ISIM): collection of IMS security data and functions on a UICC (TS 133 203 [9])

NOTE: May be a distinct application on the UICC.

integrity: See definition in TS 102 165-2 [2].

message authentication code based authentication: See definition in TS 102 165-2 [2].

PP evaluation: check if PP is complete, consistent, and technically sound (ISO/IEC 15408 [11])

Protection Profile (PP): implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs (ISO/IEC 15408-1 [12])

registrar: home of the user profile (TS 102 165-2 [2])

registry: where a PP can be stored after evaluation (ISO/IEC 15408 [11])

Service point of Attachment (SpoA): See definition in TS 102 165-2 [2].

Strength Of Function (SOF): qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms (see ISO/IEC 15408-1 [12])

Target Of Evaluation (TOE): IT product or system and its associated guidance documentation that is the subject of an evaluation (ISO/IEC 15408-1 [12])

3.2 Abbreviations

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

APE	PP evaluation (ISO/IEC 15408 [11])
AS	Application Server
ASE	Security target evaluation (ISO/IEC 15408 [11])
CA	Certification Authority
CC	Common Criteria
CNG	Customer Network Gateway
DES	TOE DEScription (ISO/IEC 15408 [11])
EAL	Evaluation Assurance Level (ISO/IEC 15408-1 [12])
ENV	Security ENVironment (ISO/IEC 15408 [11])
FE	Functional Entity

IMS	IP Multimedia Subsystem
INT	PP INTroduction (ISO/IEC 15408 [11])
ISIM	IM Subscriber Identity Module
NASS	Network Attachment SubSystem
NDS	Network Domain Security
NDS/IP	Network Domain Security for IP based protocols
NGN	TISPAN Next Generation Network
OBJ	Security OBJectives (ISO/IEC 15408 [11])
PES	PSTN/ISDN Emulation Subsystem
PKI	Public Key Infrastructure
PP	Protection Profile (ISO/IEC 15408-1 [12])
RACS	Resource and Admission Control Subsystem
REQ	IT security REQuirements, stated in ISO/IEC 15408 [11], cf. SRE
SEG	SEcurity Gateway
SF	Security Function (ISO/IEC 15408-1 [12])
SIP	Session Initiation Protocol
SOF	Strength Of Function (ISO/IEC 15408-1 [12])
SpoA	Service point of Attachment
SRE	Explicitly Stated IT REquirements, extended requirements not stated in ISO/IEC 15408 [11], cf. REQ
ST	Security Target (ISO/IEC 15408-1 [12])
T2TpoA	Transport-to-Transport point of Attachment (TS 102 165-2 [2])
TOE	Target Of Evaluation (ISO/IEC 15408-1 [12])
TSC	TSF Scope of Control (ISO/IEC 15408-1 [12])
TSF	TOE Security Functions (ISO/IEC 15408-1 [12])
TSP	TOE Security Policy (ISO/IEC 15408-1 [12])
TSS	TOE Summary Specification (ISO/IEC 15408 [11])
UE	User Equipment
UICC	Universal Integrated Circuit Card
UPSF	User Profile Server Function
VWG	Voice over IP Gateway

4 Protection profiles – NGN examples

4.1 NGN IMS Authentication Partial PP

This clause illustrates the rationale used when building the PP for NGN IP Multimedia Subsystem (IMS) authentication using the guidance from ES 202 382 [6].

4.1.1 PP Introduction

4.1.1.1 PP identification

A PP is required to provide enough labelling and descriptive information to enable it to be identified, catalogued, registered and cross referenced. The document number, version, date and full title of an ETSI standard are sufficient for this purpose and should be used.

Protection Profile					
Introduction					
Doc No.	TS 133 203	Version	v.7	Date	2005-12
Full Title	"Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services (3GPP TS 33.203 version 7.0.0 Release 7)" [9].				

4.1.1.2 PP overview

A PP should include a narrative summary as part of the Introduction. The purpose of this is to provide enough information that a potential user can make an informed decision on whether the PP is likely to be of interest. A fully specified Scope clause from an ETSI standard meets this requirement and should be used.

The existing scope and introduction from TS 133 203 [9] are quoted below:

QUOTE: *The scope for this technical specification is to specify the security features and mechanisms for secure access to the IM subsystem (IMS) for the 3G mobile telecommunication systems.*

Since the scope also encompasses the use of these security features and mechanisms for secure access to IMS in the context of fixed broadband networks, annex L specifies how the material in the main body and other normative Annexes of this document apply to the fixed broadband networks.

The IMS in UMTS will support IP Multimedia applications such as video, audio and multimedia conferences. 3GPP has chosen SIP, Session Initiation Protocol, as the signalling protocol for creating and terminating Multimedia sessions, cf. RFC 3261 (see Bibliography). This specification only deals with how the SIP signalling is protected between the subscriber and the IMS, how the subscriber is authenticated and how the subscriber authenticates the IMS.

The quoted scope statement gives a satisfactory summary of what IMS authentication offers.

Overview	The scope of the target document TS 133 203 [9] is to specify security features and mechanisms for secure access to the IM Subsystem (IMS) in TISPAN. See normative annexes other than annex L in TS 133 203 [9]. This PP identifies security functions and assurances representative of the lowest common set of requirements that should be addressed by a useful NGN-IMS. A Target Of Evaluation (TOE) compliant with this PP should meet the assurance requirements of Evaluation Assurance Level 4 (EAL4), seen as a guidance level. The IMS in UMTS will support IP Multimedia applications such as video, audio and multimedia conferences. 3GPP has chosen SIP, Session Initiation Protocol, as the signalling protocol for creating and terminating Multimedia sessions. This specification only deals with how the SIP signalling is protected between the subscriber and the IMS, how the subscriber is authenticated and how the subscriber authenticates the IMS.

4.1.2 Target Of Evaluation (TOE) description

NOTE 1: Throughout the present document, the term "Target Of Evaluation (TOE)" is used to identify any product which implements the technical requirements of the standard(s) associated with a particular PP.

ISO/IEC 15408-1 [12] requires that a brief but clear description of the Target Of Evaluation (TOE) should be included in a PP. While not expressing the security requirements in detail, this should make the security aspects of the standard clear. If the standard includes a short clause entitled "General Description" (or something similar) early in the document, it is likely that this text will be adequate as the TOE description. In the event that such a clause does not exist it will need to be written for the PP and should include the following:

- identification of the type of product that is likely to implement the standard;

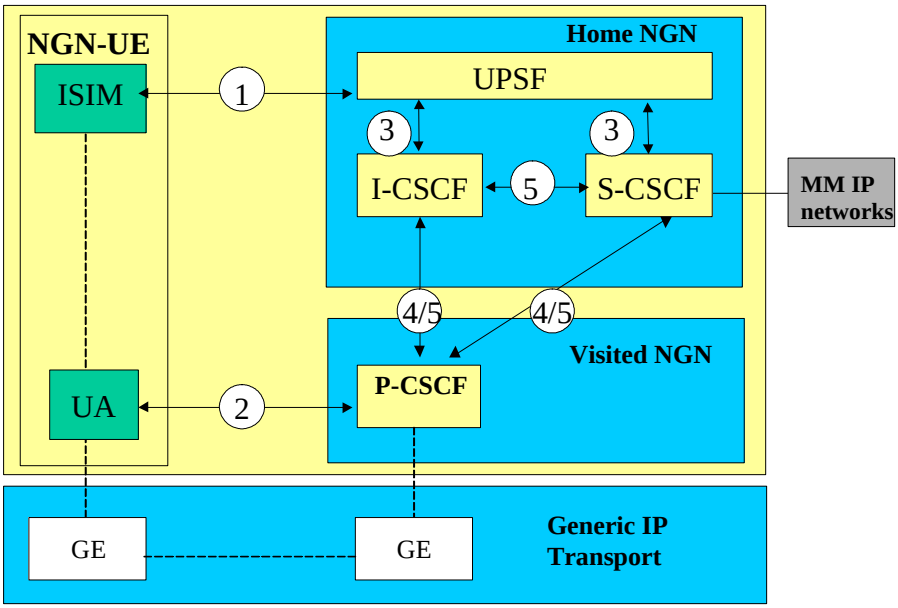
NOTE 2: In the context of the present document, the term "product" should be interpreted in its widest sense to include all types of communications equipment as well as services.

- general summary of the communications features specified in the standard or set of standards;
- brief overview of the security aspects specified in the standard.

The existing text of TS 133 203 [9] has an overview clause that provides detail of the context and services provided in the IMS domain. The text is not quoted in full as the source document is referenced by the PP itself and the full text is unnecessary to quote for that reason. Instead a précis of the text is given with the normative style of text slightly modified for the different audience.

TOE Description

In the PS domain, the service is not provided until a security association is established between the mobile equipment and the network. The IMS Security Architecture is shown in the following figure.



IMS authentication keys and functions at the user side are stored on a UICC. The IMS authentication keys and functions are designed to be logically independent to the keys and functions used for PS domain authentication. However, this does not preclude common authentication keys and functions from being used for IMS and PS domain authentication.

There are five different security associations and different needs for security protection for IMS and they are numbered 1, 2, 3, 4 and 5 in the figure of which only association 1 is considered in this PP:

1. Provides mutual authentication. The HSS delegates the performance of subscriber authentication to the S-CSCF. However the HSS is responsible for generating keys and challenges. The long-term key in the ISIM and the HSS is associated with the IMPI. The subscriber will have one (network internal) user private identity (IMPI) and at least one external user public identity (IMPU).

Mutual authentication is required between the UE and the HN.

An independent IMS security mechanism provides additional protection against security breaches. For example, if the PS-Domain security is breached the IMS would continue to be protected by its own security mechanism. As indicated in figure 1 the P-CSCF may be located either in the Visited or the Home Network. The P-CSCF shall be co-located within the same network as the GGSN, which may reside in the VPLMN or HPLMN according to the APN and GGSN selection criteria.

4.1.3 TOE security environment

The TOE security environment should describe the security aspects of the environment in which the TOE is intended to be used. It is expected to include:

- security assumptions:
  - security aspects of the environment in which an implementation of a standard will be used;
  - the intended use of the implementation;
  - the physical, user and connection aspects of the environment in which an implementation will operate;

- threats:
  - all threats against which specific protection is required within either the implementation of a standard or its expected environment;
- organizational security policies:
  - any security policies or rules with which an implementation of a standard must comply.

The TOE security environment summarizes the results of a threat analysis of the communications system specified in the base standard. Threat analyses should be prepared following the process described in TISPAN documentation.

The text of TS 133 203 [9] identifies very few assumptions or specific threats and none that would specifically suggest that authentication as a countermeasure is required.

QUOTE: (annex J of TS 133 203 [9])
After the UE does a successful SIP REGISTER with the P-CSCF, malicious UE could try to send SIP messages directly to the S-CSCF. This could imply that the UE would be able to bypass the integrity protection provided by IPSec ESP between the UE and the P-CSCF.

The reference threat analysis for TS 133 203 [9] is identified as TS 121 133 (see Bibliography) but TS 121 133 has not been specifically updated to address the IMS environment and as such there are no explicit threat analysis for IMS. However in the TISPAN NGN project some additional threat analysis of NGN aspects have been carried out to apply to TS 133 203 [9].

a TOE Security Environment		
a.1 Assumptions		
a.1.1	No specific TOE security environment assumption has been identified in the target document or in other TISPAN NGN documentation.	
a.2 Assets		
a.2.1		
a.3 Threat agents		
a.3.1	No specific TOE security environment threat agent has been identified in the target document or in other TISPAN NGN documentation.	
a.4 Threats (named in the format T.{key word(s) from textual description})		
a.4.1	T.INTERCEPT. Interception by: - Eavesdropping.	TS 102 165-1 [1] clause 5.1.2
a.4.2	T.MANIPULATE. Manipulation by: - Masquerading ("spoofing"). - Loss or corruption of information. - Unauthorized access. - Forgery.	TS 102 165-1 [1] clause 5.1.2
a.4.3	T.REPUDIATE_SEND. Repudiation of sending.	TS 102 165-1 [1] clause 5.1.2
a.4.4	T.REPUDIATE_RECEIVE. Repudiation of receiving.	TS 102 165-1 [1] clause 5.1.2
a.5 Security policies (OPTIONAL) (named in the format P.{key word(s) from textual description})		
a.5.1	P.SEPARATION. The TISPAN NGN network shall be logically and physically divided into security domains allowing for separation of application (e.g. IMS) and transport (e.g. ADSL or UMTS). Also different operators of similar networks (e.g. IMS) shall be able to operate their own security policies.	TS 187 001 [3] clause 4.1
a.5.2	P.MECHANISMS_CONFIGURABLE. Security mechanisms and other parameters beyond default security mechanisms shall be configurable. This shall be static for NNI interface and may be negotiated for UNI interfaces. The security mechanism negotiation shall have a certain minimum level to be identified by the security domain; e.g. avoid bidding-down attacks. Users shall be able to reject communications that do not conform to their minimum security policy.	TS 187 001 [3] clause 4.1
a.5.3	P.MECHANISMS_PARTITIONED. The security mechanisms shall be partitioned such that the functions of authentication, data integrity, replay detection, and confidentiality may be implemented and selected independently of each other, insofar as this makes sense.	TS 187 001 [3] clause 4.1

4.1.4 Security objectives

A PP should contain a definition of the security objectives of both the TOE and its environment. These objectives are expected to cover the assumptions, threats and policies described in the TOE security environment (see clause 4.1.3). They should be expressed in broad terms rather than in detail and should be segregated into two distinct groups, thus:

- security objectives for the TOE:
  - it should be clear which aspects of the identified threats and policies are addressed by each objective;
  - if the base security standard specifies a protocol, it is likely that the TOE security objectives will be specified in the Stage 1 (or equivalent) specification.
- security objectives for the environment:
  - it should be clear 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 TOE security objectives;
  - 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. If this is the case, the objectives should be expressed in full in the PP.

TS 133 203 [9] does not state any explicit security objectives.

b Security Objectives		
b.1 Security objectives for the TOE		
b.1.1	No specific TOE security objective has been identified in the target document or in other TISPAN NGN documentation.	
b.2 Security objectives for the environment		
b.2.1	No specific environment security objective has been identified in the target document or in other TISPAN NGN documentation.	

4.1.5 IT security requirements

4.1.5.1 The relationship between security objectives and security requirements

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. As an example, the following statement is a security objective for a TOE:

- The TOE must identify and authenticate all users before granting access to the system.

One of the security requirements associated with this objective could be:

- A user shall be successfully identified and authenticated to the TOE by means of a user name and password before all other interactions between the TOE and that user.

NOTE: It would not be unusual for a single objective to be realized by the implementation of more than one requirement nor for a single requirement to partially implement more than one objective.

4.1.5.2 TOE Security requirements

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

- TOE 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;
  - where possible, in indication of which of the functional components defined in ISO/IEC 15408-2 [13] the requirement represents.

- TOE security assurance requirements:
  - an indication of the Evaluation Assurance Level (EAL) 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 [14] which will apply to an implementation;
  - where necessary, a specification of any essential assurance requirements which are not included in ISO/IEC 15408-3 [14].

The specification of security requirements for the environment is optional and should only be included in the PP if security objectives for the environment are identified earlier in the PP (see clause 4.1.4). If requirements for the environment are included, they should be presented in the same way as functional requirements for the TOE.

This PP addresses the security assurance, and thereby the security quality, of the TISPAN target document by a focus on the security functionality as described in ISO/IEC 15408-2 [13]. Thus ISO/IEC 15408-3 [14] and security assurance as described therein does not come into play for this PP. For the end products based upon TISPAN standards the latter does play an important role to ascertain security quality and completeness.

The following are "shall" requirement quotes from the target document (excluding annexes):

QUOTE: (clause 4 of TS 133 203 [9])
IMS authentication keys and functions at the user side shall be stored on a UICC. It shall be possible for the IMS authentication keys and functions to be logically independent to the keys and functions used for PS domain authentication.

NOTE: The PS domain as stated here is to be understood as the GE domain in NGN, according to figure L.1 of TS 133 203 [9].

The following are additional requirement quotes from the target document (excluding annexes):

QUOTE: (clause 4 of TS 133 203 [9])
Mutual authentication is required between the UE and the HN.

The following are "shall" requirement quotes from TS 187 001 [3] (excluding annexes):

QUOTE: (clause 4.1, Security Policy Requirements, of TS 187 001 [3])
The TISPAN NGN network shall be logically and physically divided into securiy domains allowing for separation of application (e.g. IMS) and transport (e.g. ADSL or UMTS). Also different operators of similar networks (e.g. IMS) shall be able to operate their own security policies.

Security mechanisms and other parameters beyond default security mechanisms shall be configurable. [..] The security mechanism negotiation shall have a certain minimum level to be defined by the security domain; e.g. avoid bidding-down attacks. Users shall be able to reject communications that do not conform to their minimum security policy.

The security mechanisms shall be partitioned such that the functions of authentication, data integrity, replay detection, and confidentiality may be implemented and selected independently of each other, insofar as this makes sense.

The UE shall always offer encryption algorithms for P-CSCF to be used for the session and the P-CSCF policy shall define whether to use encryption or not.

The UE and the P-CSCF shall negotiate the integrity algorithm that shall be used for the session.

The policy of the HN shall be used to decide if an authentication shall take place for the registration of different IMPUs e.g. belonging to same or different service profiles.

QUOTE: (clause 4.2, Authentication, Authorization, Access Control and Accountability Requirements, and clause 5.3, The Core IP Multimedia Subsystem (IMS), of TS 187 001 [3])
Access to NGN networks, services, and applications shall be provided for authorized users only.

In non-early deployment scenarios, IMS authentication shall be independent from access authentication.

An ISIM shall be used to access any IMS service, however, exeptions may be allowed for emergency calls and early deployment scenarios.

ISIM based Re-authentication of an IMS-subscriber and the network shall comply to the authentication part of Access Security for IP-based services TS 133 203 [9].

ISIM based Re-authentication of an IMS-subscriber shall comply to the authentication part of Access Security for IP-based services TS 133 203 [9].

It shall be possible to prevent the use of a particular ISIM to access NGN networks and services and it should be possible to revoke a specific ISIM.

NGN relevant ISIM specific information shall be protected against5 unauthorized access or alteration.

User Authentication to the NGN IMS using SIP Digest mechanisms shall be supported as an early deployment scenario.

Where both Digest and ISIM solutions are deployed by an NGN IMS operator, that operator shall determine the authentication mechanism (SIP Digest or ISIM-based) on a per-user basis. The authentication mechanism shall be enforced according to both the subscription information in the user' s service profile and the specific policies of the NGN operator.

Transmitted passwords shall be sufficiently protected; e.g. by encryption or other techniques.

For the special early deployment scenarios [..], where IMS authentication is linked to access authentication, it shall be possible to gain access to IMS services after an authentication procedure.

The NGN subsystems shall be able to [..] define and enforce policy with respect to validity of user authorization.

In case the CNG is a routing modem and the Customer Premises Network (CPN) is a private OP realm, authentication shall be initiated from the NGN.

Authentication of NGN users and authentication of NGN terminals shall be separate.

Caller id and location information shall be stored according to the Common European regulatory framework by the EMTEL Service Provider. Caller ID and location information shall be validated by the EMTEL Service provider.

The TISPAN NGN network shall be logically and physically divided into security domains allowing for separation of applications (e.g. IMS) and transport (e.g. ADSL or UMTS). Also different operators of similar networks (e.g. IMS) shall be able to operate their own security policies.

Security mechanisms and other parameters beyond default security mechanisms shall be configurable. This shall be static for NNI interface and may be negotiated for UNI interfaces. The security mechanism negotiation shall have a certain minimum level to be defined by the security domain; e.g. avoid bidding-down attacks. Users shall be able to reject communications that do not conform to their minimum security policy.

The security mechanisms shall be partitioned such that the functions of authentication, data integrity, replay detection, and confidentiality may be implemented and selected independently of each other, insofar as this makes sense.

The UE shall always offer encryption algorithms for P-CSCF to be used for the session and the P-CSCF policy shall define whether to use encryption or not.

The UE and the P-CSCF shall negotiate the integrity algorithm that shall be used for the session.

The policy of the HN shall be used to decide if an authentication shall take place for the registration of different IMPUs, e.g. belonging to same or different service profiles.

QUOTE: (clause 4.3, Identity and Secure Registration Requirements, and clause 5.3, The Core IP Multimedia Subsystem (IMS), of TS 187 001 [3])

It shall be possible to implicitly register IMPU(s). [..] All the IMPU(s) being implicitly registered shall be delivered by the HSS to the S-CSCF and subsequently to the P-CSCF. The S-CSCF shall regard all implicitly registered IMPU(s) as registered IMPU(s).

An access identity shall be used for access authentication.

QUOTE: (clause 4.4.1, General Communications and Data Security Requirements, and clause 5.3, The Core IP Multimedia Subsystem (IMS), of TS 187 001 [3])

An ISIM based solution for IMS access security (authentication, confidentiality and integrity protection) of signalling to and from the user, shall be supported.

In the case where IMS authentication is linked to access line authentication the underlying access technology shall provide protection of NGN signalling and user data.

ISIM specific information shall be updated in a secure manner.

QUOTE: (clause 4.4.2, Integrity and Replay Protection Requirements, and clause 5.3, The Core IP Multimedia Subsystem (IMS), of TS 187 001 [3])

It shall be possible to ensure the origin, integrity and freshness of authentication data, particularly of the cipher key.

Some of the quoted requirements have been incorporated in the partial PP, see table below.

c IT Security Requirements			
c.1 TOE security requirements			
c.1.1 TOE security functional requirements (named in the format R.{key word(s) from textual description})			
c.1.1.1	R.LEGACY. NGN R1 IMS authentication shall support early deployment scenarios (with support for legacy equipments).	FIA_UAU.3	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2
c.1.1.2	R.INDEPENDENT. In non-early deployment scenarios, IMS authentication shall be independent from access authentication.	FIA_UAU.3	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2
c.1.1.3	R.ISIM_AUTHENTICATION. ISIM based Authentication between the IMS-subscriber and the network shall comply to the authentication part of Access Security for IP-based services TS 133 203 [9].	FIA_UAU.4	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2
c.1.1.4	R.ISIM_REAUTHENTICATION. ISIM based Re-authentication of an IMS-subscriber shall comply to the authentication part of Access Security for IP-based services TS 133 203 [9].	FIA_UAU.6	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2
c.1.1.5	R.ISIM_COMPLIANCE. ISIM based Re-authentication of an IMS-subscriber shall comply to the authentication part of Access Security for IP-based services TS 133 203 [9]	FIA_UAU.6	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2
c.1.1.6	R.SIP. User Authentication to the NGN IMS using SIP Digest mechanisms shall be supported as an early deployment scenario.	FIA_UAU.4	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2
c.1.1.7	R.SIP_AND_ISIM. Where both Digest and ISIM solutions are deployed by an NGN IMS operator, that operator shall determine the authentication mechanism (SIP Digest or ISIM-based) on a per-user basis. The authentication mechanism shall be enforced according to both the subscription information in the user's service profile and the specific policies of the NGN IMS operator.	FIA_UAU.4	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2
c.1.1.8	R.PASSWORDS. Transmitted passwords shall be sufficiently protected; e.g. by encryption or other techniques.	FDP_DAU.1, FIA_UAU.3	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clauses 10.3.2 and 11.4.2
c.1.1.9	R.EARLY_DEPLOYMENT. For the special early deployment scenarios, where IMS authentication is linked to access authentication, it shall be possible to gain access to IMS services after an authentication procedure. This authentication provides simultaneous access to the access network and IMS services.	FIA_UAU.4	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2
c.1.2 TOE security assurance requirements			
c.1.2.1	Not applicable		
c.2 Environment security requirements (OPTIONAL)			
c.2.1	Not applicable		

4.1.6 Application notes (OPTIONAL)

ISO/IEC 15408-1 [12] provides for optional application notes to be included in a PP. It is intended that this should include any additional information that might be considered useful to either or both of the implementor and the evaluator. This clause should be unnecessary if the base security standard has been fully and carefully specified.

d Application notes (OPTIONAL)
Not applicable

4.1.7 Rationale

ISO/IEC 15408-1 [12] requires that a PP provides a rationale, subdivided into security objectives rationale and security requirements rationale to explain in detail how the security objectives and the security requirements, respectively, address the threats identified in the TOE security environment. This rationale should be included in the Vulnerability Analysis.

e Rationale
Not applicable

4.2 NGN-NDS Source Authentication Partial PP

This clause illustrates the rationale used when building the PP for NGN Network Domain Security (NDS) authentication using the guidance from ES 202 382 [6].

4.2.1 PP Introduction

4.2.1.1 PP identification

A PP is required to provide enough labelling and descriptive information to enable it to be identified, catalogued, registered and cross referenced. The document number, version, date and full title of an ETSI standard are sufficient for this purpose and should be used.

Protection Profile					
Introduction					
Doc No.	TS 133 210	Version	v.7	Date	2005-12
Full Title	"Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 version 7.0.0 Release 7)" [10].				

4.2.1.2 PP overview

A PP should include a narrative summary as part of the Introduction. The purpose of this is to provide enough information that a potential user can make an informed decision on whether the PP is likely to be of interest. A fully specified Scope clause from an ETSI standard meets this requirement and should be used.

The existing scope and introduction from TS 133 210 [10] are quoted below:

QUOTE:

The present document defines the security architecture for network domain IP based control planes, which shall be applied to NDS/IP-networks (i.e. 3GPP and fixed broadband networks). The scope of network domain control plane security is to cover the control signalling on selected interfaces between network elements of NDS/IP networks.

The scope [.....] is to outline the basic principles for the network domain security architecture. A central concept introduced in this specification is the notion of a security domain. The security domains are networks that are managed by a single administrative authority. Within a security domain the same level of security and usage of security services will be typical. Typically, a network operated by a single operator will constitute one security domain although an operator may at will subsection its network into separate sub-networks.

The quoted scope statement gives a satisfactory summary of what IMS authentication offers.

Overview	The target document defines the security architecture for network domain IP based control planes, which shall be applied to NDS/IP-networks (i.e. 3GPP and fixed broadband networks). The scope of network domain control plane security is to cover the control signalling on selected interfaces between network elements of NDS/IP networks. This PP identifies security functions and assurances representative of the lowest common set of requirements that should be addressed by a useful NGN-NDS. A Target Of Evaluation (TOE) compliant with this PP should meet the assurance requirements of Evaluation Assurance Level 4 (EAL4), seen as a guidance level. The scope of the target document TS 133 210 [10] is to outline the basic principles for the network domain security architecture. A central concept introduced in the target document is the notion of a security domain. The security domains are networks that are managed by a single administrative authority. Within a security domain the same level of security and usage of security services will be typical. Typically, a network operated by a single operator will constitute one security domain although an operator may at will subsection its network into separate sub-networks.

4.2.2 Target Of Evaluation (TOE) description

NOTE 1: Throughout the present document, the term "Target Of Evaluation (TOE)" is used to identify any product which implements the technical requirements of the standard(s) associated with a particular PP.

ISO/IEC 15408-1 [12] requires that a brief but clear description of the Target Of Evaluation (TOE) should be included in a PP. While not expressing the security requirements in detail, this should make the security aspects of the standard clear. If the standard includes a short clause entitled "General Description" (or something similar) early in the document, it is likely that this text will be adequate as the TOE description. In the event that such a clause does not exist it will need to be written for the PP and should include the following:

- identification of the type of product that is likely to implement the standard;

NOTE 2: In the context of the present document, the term "product" should be interpreted in its widest sense to include all types of communications equipment as well as services.

- general summary of the communications features specified in the standard or set of standards;
- brief overview of the security aspects specified in the standard.

The existing text of TS 133 210 [10] has descriptive clauses that provide information about the context and services provided in the NDS domain (TS 133 210 [10] clauses 4.2, 4.3 and 4.5). The text is not quoted in full as the source document is referenced by the PP itself.

TOE Description
The network domain control plane of an NDS/IP network is sectioned into security domains which typically coincide with operator borders. The border between the security domains is protected by Security Gateways (SEGs). The SEGs are responsible for enforcing the security policies towards other SEGs and for the interworking of networks. SEGs are designed to handle communication over the Za interface. The security may include filtering policies and firewall functionality not specified in the target document TS 133 210 [10]. This PP addresses communication between a Security Gateway (SEG) in one NDS and another SEG in a neighbouring NDS. The setup is depicted in the figure (based upon TS 133 210 [10] clause 5). In NDS the IPsec security protocol shall always be ESP (TS 133 210 [10] clause 5.1). In NDS it is mandated that integrity protection/message authentication, together with anti-replay protection, shall always be used. The security services provided by NDS/IP are (TS 133 210 [10] clause 5.1): • Data integrity. • Data origin authentication. • Anti-replay protection. • Confidentiality (OPTIONAL). There is limited protection against traffic flow analysis when confidentiality is applied. The PP covers the use of the data origin authentication service only. For native IP-based protocols, security is provided at the network layer. The security protocols used at the network layer are the IETF defined IPsec security protocols as specified in RFC 2401 [16]. The network domain security of an NDS/IP network does not extend to the user plane. Consequently, the security domains and the associated SEGs do not encompass the user plane Gi interface towards other, possibly external, IP networks. A chained-tunnel/hub-and-spoke approach is used. This facilitates hop-by-hop based security protection. All NDS/IP traffic passes through a SEG before entering or leaving the security domain. SEGs are physically secured and offer secure storage of long-term keys used for IKE authentication.

4.2.3 TOE security environment

The TOE security environment should describe the security aspects of the environment in which the TOE is intended to be used. It is expected to include:

- security assumptions:
  - security aspects of the environment in which an implementation of a standard will be used;
  - the intended use of the implementation;
  - the physical, user and connection aspects of the environment in which an implementation will operate;
- threats:
  - all threats against which specific protection is required within either the implementation of a standard or its expected environment;
- organizational security policies:
  - any security policies or rules with which an implementation of a standard must comply.

The TOE security environment summarizes the results of a threat analysis of the communications system specified in the base standard. Threat analyses should be prepared following the process described in TISPAN documentation.

The text of TS 133 210 [10] identifies assumptions (some of these can be seen as requirements, but have been phrased in this PP to become assumptions) and policies. However, specific threats have not been identified. It is specified in the target document that data origin authentication as a countermeasure is a security service provided by NDS/IP (TS 133 210 [10] clause 5.1). Some quotes from the target document are given here (taken from TS 133 210 [10] clause 4 only, for a more complete list see the table below).

QUOTE: (clause 4.2 of TS 133 210 [10])
The security protocols to be used at the network layer are the IETF defined IPsec security protocols as specified in RFC-2401.

QUOTE: (clause 4.3 of TS 133 210 [10])
The network domain control plane of an NDS/IP-network is sectioned into security domains and typically these coincide with operator borders. The border between the security domains is protected by Security Gateways (SEGs). The SEGs are responsible for enforcing the security policy of a security domain towards other SEGs in the destination security domain. The network operator may have more than one SEG in its network in order to avoid a single point of failure or for performance reasons. A SEG may be defined for interaction towards all reachable security domain destinations or it may be defined for only a subset of the reachable destinations.

The network domain security of an NDS/IP-network does not extend to the user plane and consequently the security domains and the associated security gateways towards other domains do not encompass the user plane Gi-interface towards other, possibly external, IP networks.

A chained-tunnel/hub-nad-spoke approach is used which facilitates hop-by-hop based security protection.

QUOTE: (clause 4.5 of TS 133 210 [10])
Security Gateways (SEGs) [...] will be used for securing native IP based protocols. The SEGs are defined to handle communication over the Za-interface, which is located between SEGs from different IP security domains.

The number of SEGs in a security domain will depend on the need to differentiate between the externally reachable destinations, the need to balance traffic and to avoid single points of failure. The security may include filtering policies and firewall functionality not required in this specification.

For security "shall" statements in these clauses, see quotes in clause 4.2.5.2.

The information identified in the target document TS 133 210 [10] as being related to assumptions, threats and policies has been structured and phrased into the PP assumption, threat and policy entries in the table below.

a TOE Security Environment		
a.1 Assumptions (named in the format A.{key word(s) from textual description})		
a.1.1	A.SECURITY_DOMAINS. The network domain control plane of an NDS/IP network is physically and logically sectioned into security domains. Typically these coincide with operator borders.	TS 133 210 [10] clauses 4.3 and 4.4.1
a.1.2	A.BORDER_PROTECTION. The border between security domains is protected by Security Gateways (SEGs).	TS 133 210 [10] clauses 4.3 and 4.5
a.1.3	A.SEG_ENFORCING. A SEG is responsible for enforcing the security policy of a security domain towards another SEG in a destination security domain, and for the interworking between these networks. The security may include filtering policies and firewall functionality.	TS 133 210 [10] clauses 4.3, 4.5 and 5.6.1
a.1.4	A.SEG_NUMBER. A security domain can have one or more SEGs, depending on the need to differentiate between the externally reachable destinations, the need to balance the traffic load, to avoid single points of failure, or for performance reasons.	TS 133 210 [10] clauses 4.3 and 4.5
a.1.5	A.SEG_REACHABILITY. A SEG may be defined for interaction towards all reachable security domains, or it may be defined for only a subset of the reachable destinations. A SEG handles NDS/IP traffic in or out of a security domain, towards a well-defined set of other (reachable) IP security domains.	TS 133 210 [10] clauses 4.3, 4.5 and 5.6.1
a.1.6	A.USER_PLANE. The network domain security of an NDS/IP network does not extend to the user plane. The consequence is that the security domains and the associated SEGs towards other domains do not encompass the user interface Gi towards other, possibly external, IP networks.	TS 133 210 [10] clause 4.3
a.1.7	A.HOP_BY_HOP. A chained-tunnels or hub-and-spoke approach is used to facilitate hop-by-hop based security protection.	TS 133 210 [10] clauses 4.3 and 5.6.1
a.1.8	A.SEG_SECURES_NATIVE_IP. A SEG secures native IP based protcols.	TS 133 210 [10] clause 4.5
a.1.9	A.SEG_OVER_ZA_IF. A SEG handles communication over Za interface, located between SEGs in different IP security domains.	TS 133 210 [10] clauses 4.5 and 5.6.2
a.1.10	A.IPSEC_SA. IPsec offers a set of security services, which is determined by the negotiated IPsec Security Associations (IPsec SAs). The IPsec SAs define which security protocol to be used, the mode and the end points of the SA.	TS 133 210 [10] clause 5.1
a.1.11	A.IKE. For NDS/IP networks the key management and distribution between SEGs is handled by the protocol Internet Key Exchange (IKE).	TS 133 210 [10] clause 5.2, RFC 2407 [17], RFC 2408 [18], RFC 2409 [19]
a.1.12	A.TUNNEL_MODE_SUPPORT. NDS/IP only requires support for tunnel mode IPsec SAs.	TS 133 210 [10] clause 5.2
a.1.13	A.ESP_SA_SUPPORT. NDS/IP only requires support for ESP SAs.	TS 133 210 [10] clause 5.2
a.1.14	A.NEGOTIATE_BUNDLES. There is no need to be able to negotiate IPsec SA bundles since a single ESP SA is sufficient to set up to protect traffic between nodes.	TS 133 210 [10] clause 5.2
a.1.15	A.SPD_INSTRUMENT. The Security Policy Database (SPD) is a policy instrument to decide which security services are to be offered and in what fashion.	TS 133 210 [10] clause 5.2.1
a.1.16	A.SPD_ROLE. The SPD plays a central role when defining security policies, both within the internal security domain and towards external security domains. The security policy towards external security domains is subject to roaming agreements.	TS 133 210 [10] clause 5.2.1
a.1.17	A.SAD_PARAMETERS. The Security Association Database (SAD) contains parameters that are associated with the active security associations. Every SA has an entry in the SAD.	TS 133 210 [10] clause 5.2.2
a.1.18	A.SAD_OUTBOUND. For outbound processing, a lookup in the SPD points to an entry in the SAD.	TS 133 210 [10] clause 5.2.2
a.1.19	A.RANDOM_DATA. NDS/IP contains element(s) that can generate random data (for IV).	TS 133 210 [10] clause 5.3.5, RFC 1750 [15]

a.2	Assets	
a.2.1		
a.3	Threat agents	
a.3.1	No specific TOE security environment threat agent has been identified in the target document or in other TISPAN NGN documentation.	
a.4	Threats (named in the format T.{key word(s) from textual description})	
a.4.1	T.INTERCEPT. Interception by eavesdropping.	TS 102 165-1 [1] clause 5.1.2
a.4.2	T.MANIPULATE. Manipulation by : - Masquerading (spoofing). – Loss or corruption of information. – Unauthorized access. – Forgery.	TS 102 165-1 [1] clause 5.1.2
a.4.3	T.REPUDIATE_SEND. Repudiation of sending.	TS 102 165-1 [1] clause 5.1.2
a.4.4	T.REPUDIATE_RECEIVE. Repudiation of receiving.	TS 102 165-1 [1] clause 5.1.2
a.5	Security policies (OPTIONAL) (named in the format P.{key word(s) from textual description})	
a.5.1	P.POLICY_DATABASE. Security Policy Database (SPD) is a policy instrument to decide which services are to be offered and in what fashion.	TS 133 210 [10] clause 5.2.1
a.5.2	P.IN_OUTBOUND. SPD shall be consulted during processing of both inbound and outbound traffic. Includes traffic not protected by IPsec. SPD must have unique entries for inbound and outbound traffic so that SPD can discriminate among traffic protected by IPsec, bypassing IPsec, or discarded by IPsec.	TS 133 210 [10] clause 5.2.1
a.5.3	P.GRANULARITY. Policy control granularity afforded by NDS/IP is determined by degree of control with respect to ESP Security Association between NEs and SEGs. Normal mode of operation is that only one ESP SA is used between any two NEs or SEGs. Therefore the security policy is identical to all secured traffic passing between NEs.	TS 133 210 [10] clause 5.5
a.5.4	P.INTRA_DOMAIN. Security domains should have the same security policy in force for all traffic within the security domain.	TS 133 210 [10] clause 5.5
a.5.5	P.INTER_DOMAIN. The inter-security domain policy is determined by roaming agreements when security domains belong to different operators.	TS 133 210 [10] clause 5.5, TS 187 001 [3] clause 4.1
a.5.6	P.IPSEC_SEG. IPsec security policy enforcement for inter-security domain communication is a matter for SEGs of communicating security domains.	TS 133 210 [10] clause 5.5

4.2.4 Security objectives

A PP should contain a definition of the security objectives of both the TOE and its environment. These objectives are expected to cover the assumptions, threats and policies described in the TOE security environment (see clause 4.2.3). They should be expressed in broad terms rather than in detail and should be segregated into two distinct groups, thus:

- security objectives for the TOE:
  - it should be clear which aspects of the identified threats and policies are addressed by each objective;
  - if the base security standard specifies a protocol, it is likely that the TOE security objectives will be specified in the Stage 1 (or equivalent) specification.
- security objectives for the environment:
  - it should be clear 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 TOE security objectives;
  - 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. If this is the case, the objectives should be expressed in full in the PP.

b Security Objectives		
b.1	Security objectives for the TOE (named in the format O.{key word(s) from textual description})	
b.1.1	O.BI-DIRECTIONAL. To secure bi-directional communication between two SEGs.	TS 133 210 [10] clause 5.2
b.2	Security objectives for the environment (named in the format OE.{key word(s) from textual description})	
b.2.1	OE.SEG B_BI-DIRECTIONAL. To secure bi-directional communication between two SEGs - in other network.	TS 133 210 [10] clause 5.2

4.2.5 IT security requirements

4.2.5.1 The relationship between security objectives and security requirements

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. As an example, the following statement is a security objective for a TOE:

- The TOE must identify and authenticate all users before granting access to the system.

One of the security requirements associated with this objective could be:

- A user shall be successfully identified and authenticated to the TOE by means of a user name and password before all other interactions between the TOE and that user.

NOTE: It would not be unusual for a single objective to be realized by the implementation of more than one requirement nor for a single requirement to partially implement more than one objective.

4.2.5.2 TOE security requirements

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

- TOE 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;
  - where possible, in indication of which of the functional components defined in ISO/IEC 15408-2 [13] the requirement represents.
- TOE security assurance requirements:
  - an indication of the Evaluation Assurance Level (EAL) 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 [14] which will apply to an implementation;
  - where necessary, a specification of any essential assurance requirements which are not included in ISO/IEC 15408-3 [14].

The specification of security requirements for the environment is optional and should only be included in the PP if security objectives for the environment are identified earlier in the PP (see clause 4.2.4). If requirements for the environment are included, they should be presented in the same way as functional requirements for the TOE.

The following are "shall" requirement quotes from the target document (excluding annexes):

NOTE: A number of additional "shall" requirements have been taken from TS 187 001 [3].

QUOTE: (clause 4.3 of TS 133 210 [10])
All NDS/IP traffic shall pass through a SEG before entering or leaving the security domain.

QUOTE: (clause 4.4 of TS 133 210 [10])
The network domain of an NDS/IP-network shall be logically and physically divided into security domains. These control plane security domains may closely correspond to the core network of a single operator and shall be separated by means of security gateways.

QUOTE: (clause 4.5 of TS 133 210 [10])
All NDS/IP traffic shall pass through a SEG before entering or leaving the security domain. Each security domain can have one or more SEGs.

The security gateways shall be responsible for enforcing security policies for the interworking between networks.

SEGs are responsible for security operations and shall be physically secured. They shall offer capabilities for secure storage of long-term keys used for IKE authentication.

QUOTE: (clause 5.1 of TS 133 210 [10])
For NDS/IP-networks the IPsec security protocol shall always be ESP. For NDS/IP-networks it is further mandated that integrity protection/message authentication together with anti-replay protection shall always be used.

QUOTE: (clause 5.2.1 of TS 133 210 [10])
The SPD shall be consulted during processing of both inbound and outbound traffic. This also includes traffic that shall not/need not be protected by IPsec. In order to achieve this the SPD must have unique entries for both inbound and outbound traffic such that the SPD can discriminate among the traffic that shall be protected by IPsec, that shall bypass IPsec or that shall be discarded by IPsec.

QUOTE: (clause 5.2.2 of TS 133 210 [10])
If an SPD entry does not point to an SA that is appropriate for the packet, an SA shall be automatically created.

QUOTE: (clause 5.3.1 of TS 133 210 [10])
When NDS/IP is applied, only the ESP (RFC-2406 [..]) security protocol shall be used for all NDS/IP inter-domain control plane traffic.

QUOTE: (clause 5.3.2 of TS 133 210 [10])
Since security gateways are an integral part of the NDS/IP architecture, tunnel mode shall be supported. For NDS/IP inter-domain communication, security gateways shall be used and consequently only tunnel mode (RFC-2401 [..]) is applicable for this case.

QUOTE: (clause 5.3.3 of TS 133 210 [10])
It is therefore explicitly noted that for use in NDS/IP, the ESP_DES transform shall not be used and instead it shall be mandatory to support the ESP_3DES transform.

It is noted that the AES-CBC key length for use with this specification shall be 128 bits.

QUOTE: (clause 5.3.4 of TS 133 210 [10])
For NDS/IP traffic ESP shall always be used to provide integrity, data origin authentication, and anti-replay services, thus the ESP_NULL authentication algorithm is explicitly not allowed for use. ESP shall support ESP_HMAC_SHA-1 algortihm in NDS/IP.

QUOTE: (clause 5.3.5 of TS 133 210 [10])
The following strengthening of the requirements on how to construct the IV shall take precedence over the description given in the implementation note in RFC-2405 [..] section 5, the description given in RFC-2451 [..] section 3 and all other descriptions that allow for predictable IVs.

The IV field shall be the same size as the block size of the cipher algorithm being used. The IV shall be chosen at random, and shall be unpredictable to any party other than the originator.

QUOTE: (clause 5.4 of TS 133 210 [10])
The Internet Key Exchange protocol shall be used for negotiation of IPsec SAs. The following additional requirement on IKE is made mandatory for inter-security domain SA negotiations over the Za-interface.

For IKE phase-1 (ISAKMP SA):

- The use of pre-shared secrets for authentication shall be supported;

- Only Main Mode shall be used;

- IP addresses and Fully Qualified Domain Names (FQDN) shall be supported for identification;

- Support of 3DES in CBC mode shall be mandatoryfor confidentiality;

- Support of AES in CBC mode (RFC-3602 [..]) shall be mandatory for confidentiality;

- Support of SHA-1 shall be mandatory for integrity/message authentication;

- Support of Diffie-Hellman group 2 shall be mandatory for Diffie-Hellman exchange.

Phase-1 IKE SAs shall be persistent with respect to the IPsec SAs is derived from it. That is, IKE SAs shall have a lifetime for at least the same duration as does the derived IPsec SAs.

The elapsed time between the new SA establishment and the cancellation of the old SA shall be sufficient to avoid losing any data being transmitted within the old SA.

For IKE phase-2 (IPsec SA):

- [..]

- Only IP addresses or subnet identity types shall be mandatory address types;

- Support of Notifications shall be mandatory;

- Support of Diffie-Hellman group 2 shall be mandatory for Diffie-Hellman exchange.

It is noted that the key length for use with this specification shall be 128 bits.

QUOTE: (clause 5.6.1 of TS 133 210 [10])
In NDS/IP only the Security Gateways (SEGs) shall engage in direct communication with entities in other security domains for NDS/IP traffic.

QUOTE: (clause 5.6.2 of TS 133 210 [10])
All security domains compliant with this specification shall operate the Za-interface.

The following are additional requirement quotes from the target document:

QUOTE: (clause 4.2 of TS 133 210 [10])
The security protocols to be used at the network layer are the IETF defined IPsec security protocols as specified in RFC-2401 [..].

QUOTE: (clause 5.2 of TS 133 210 [10])
To secure typical, bi-directional communication between two hosts, or between two security gateways an ISAKMP Security Associations and two IPsec Security Associations (one in each direction) are required.

NDS/IP only requires support for ISAKMP SAs with pre-shared keys.

QUOTE: (clause 5.3.3 of TS 133 210 [10])
Support for the AES-CBC cipher algorithm (RFC-3602 [..]) is mandatory.

QUOTE: (clause 5.3.5 of TS 133 210 [10])
It is explicitly not allowed to construct the IV from the encrypted data of the preceding encryption process.

[..] These requirements imply that the network must have a capability to generate random data.

QUOTE: (clause 5.4 of TS 133 210 [10])
Since the AES-CBC allows variable key lengths, the Key Length attribute must be specified in both a Phase 1 exchange [..] and a Phase 2 exchange [..].

The following are "shall" requirement quotes from TS 187 001 [3]:

QUOTE: (clause 4.1, Security Policy Requirements, of TS 187 001 [3])
The TISPAN NGN network shall be logically and physically divided into security domains allowing for separation of application (e.g. IMS) and transport (eg. ADSL or UMTS). Also different operators of similar networks (e.g. IMS) shall be able to operate their own security policies.

Security mechanisms and other parameters beyond default security mechanisms shall be configurable. [..].The security mechanism negotiation shall have a certain minimum level to be defined by the security domain; e.g. avoid bidding-down attacks. Users shall be able to reject communications that do not conform to their minimum security policy.

The security mechanisms shall be partitioned such that the functions of authentication, data integrity, replay detection, and confidentiality may be implemented and selected independently of each other, insofar as this makes sense.

The security gateway functions (SEGF) shall be responsible for enforcing security policies for the interworking between networks.

SEGFs are responsible for security sensitive operations and shall offer capabilities for secure storage of long-term keys used for IKE authentication.

QUOTE: (clause 4.4.1, General Communications and Data Security Requirements, of TS 187 001 [3])
*Network Domain Security (NDS) shall be provided at the network layer and comply to TS 133 210 [*10*].*

*All NDS/IP traffic shall pass through a SEGF (Security gateway Function) before entering or leaving the security domain. IMS operators shall operate NDS/IP Za interface between SEGFs according to TS 133 210 [*10*].*

QUOTE: (clause 4.6, Key Management Requirements, of TS 187 001 [3])
*Key management and key distribution between SEGFs shall comply to the Network Domain Security TS 133 210 [*10*].*

Some of the quoted requirements have been incorporated in the partial PP, see table below.

c IT Security Requirements			
c.1 TOE security requirements			
c.1.1 TOE security functional requirements (named in the format R.{key word(s) from textual description})			
c.1.1.1	R.IMPLEMENT_IPSEC_SA. Secure bi-directional communication between two SEGs shall be established using two IPsec Security Associations (one in each direction)	FDP_UCT.1, FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MSA.1(1), FMT_MSA.1(2), and FMT_MSA.2	TS 133 210 [10] clause 5.4, ISO/IEC 15408-2 [13] clauses 10.12.2, 10.13.2, 12.1.2 and 12.2.2
c.1.1.2	R.IMPLEMENT_ISAKMP_SA. Secure bi-directional communication between two SEGs shall be established using an ISAKMP Security Association	FDP_UCT.1, FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MSA.1(1), FMT_MSA.1(2), and FMT_MSA.2	TS 133 210 [10] clause 5.4, ISO/IEC 15408-2 [13] clauses 10.12.2, 10.13.2, 12.1.2 and 12.2.2
c.1.1.3	R.ESP_3DES. ESP 3DES (CBC) encryption transform shall be supported	FDP_UCT.1, FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MSA.1(1), FMT_MSA.1(2) and FMT_MSA.2	TS 133 210 [10] clauses 5.1, 5.3.1, 5.3.3 and 5.4, ISO/IEC 15408-2 [13] clauses 10.12.2, 10.13.2, 12.1.2 and 12.2.2
c.1.1.4	R.SPD. The SPD shall be consulted during processing of both inbound and outbound traffic	FDP_DAU.1, FDP_DAU.2, FDP_SDI.1, FDP_SDI.2, FDP_UCT.1, FDP_UIT.1, FDP_UIT.2 and FDP_UIT.3	TS 133 210 [10] clause 5.2.1, ISO/IEC 15408-2 [13] clauses 10.3.2, 10.11.2, 10.12.2 and 10.13.2
c.1.1.5	R.SAD. An SA shall be automatically created if an SPD entry does not point to an SA that is appropriate for the packet	FDP_DAU.1, FDP_DAU.2, FDP_SDI.1, FDP_SDI.2, FDP_UCT.1, FDP_UIT.1, FDP_UIT.2 and FDP_UIT.3	TS 133 210 [10] clause 5.2.2, ISO/IEC 15408-2 [13] clauses 10.3.2, 10.11.2, 10.12.2 and 10.13.2

c.1.1.6	R.AES_CBC. AES CBC cipher algorithm shall be supported	FDP_UCT.1, FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MSA.1(1), FMT_MSA.1(2) and FMT_MSA.2	TS 133 210 [10] clauses 5.3.3 and 5.4, ISO/IEC 15408-2 [13] clauses 10.12.2, 10.13.2, 12.1.2 and 12.2.2
c.1.1.7	R.ESP_AUTHENTICATION. ESP_HMAC_SHA-1 authentication transform shall be supported	FDP_UCT.1, FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MSA.1(1), FMT_MSA.1(2) and FMT_MSA.2	TS 133 210 [10] clauses 5.2, 5.3.4 and 5.4, ISO/IEC 15408-2 [13] clauses 10.12.2, 10.13.2, 12.1.2 and 12.2.2
c.1.1.8	R.IV_RANDOM. Random data generation capability for IV shall be supported	FDP_UCT.1, FDP_UIT.2 and FDP_UIT.3	TS 133 210 [10] clause 5.3.5, RFC 1750 [15], ISO/IEC 15408-2 [13] clauses 10.12.2 and 10.13.2
c.1.1.9	R.ENFORCE_POLICIES. The security gateway functions (SEGF) shall be responsible for enforcing security policies for the interworking between networks	FPT_FLS.1, FPT_ITA.1, FPT_ITC.1, FPT_ITI.1, FPT_PHP.3, FPT_RCV.4, FPT_RPL.1, FPT_RVM.1, FPT_SEP.3, FPT_SSP.2, FPT_TDC.1, FPT_TST.1	TS 133 210 [10] clause 4.5, TS 187 001 [3] clause 4.1, ISO/IEC 15408-2 [13] clauses 14.2.2, 14.3.2, 14.4.2, 14.5.2, 14.7.2, 14.8.2, 14.9.2, 14.10.2, 14.11.2, 14.12.2, 14.14.2, 14.16.2
c.1.1.10	R.SECURE_STORAGE. SEGFs are responsible for security sensitive operations and shall offer capabilities for secure storage of long-term keys used for IKE authentication	FPT_FLS.1, FPT_ITA.1, FPT_PHP.3, FPT_RCV.4	TS 133 210 [10] clause 4.5, TS 187 001 [3] clause 4.1, ISO/IEC 15408-2 [13] clauses 14.2.2, 14.3.2, 14.7.2, 14.8.2
c.1.1.11	R.NDS. Network Domain Security (NDS) shall be provided at the network layer and comply to TS 133 210 [10]	FPT_FLS.1, FPT_ITA.1, FPT_ITC.1, FPT_ITI.1, FPT_RPL.1, FPT_RVM.1, FPT_SEP.3, FPT_SSP.2, FPT_TDC.1, FPT_TST.1	TS 187 001 [3] clause 4.4.1, ISO/IEC 15408-2 [13] clauses 14.2.2, 14.3.2, 14.4.2, 14.5.2, 14.7.2, 14.10.2, 14.11.2, 14.12.2, 14.14.2, 14.16.2
c.1.1.12	R.SEGF. All NDS/IP traffic shall pass through a SEG, Security Gateway (SEGF, Security Gateway Function) before entering or leaving the security domain.	FPT_RVM.1	TS 133 210 [10] clauses 4.3 and 4.5, TS 187 001 [3] clause 4.4.1, ISO/IEC 15408-2 [13] clause 14.10.2
c.1.1.13	R.ZA_INTERFACE. IMS operators shall operate NDS/IP Za interface between SEGFs according to TS 133 210 [10]	FPT_ITA.1, FPT_ITC.1, FPT_ITI.2	TS 187 001 [3] clause 4.4.1, ISO/IEC 15408-2 [13] clauses 14.3.2, 14.4.2, 14.5.2
c.1.1.14	R.KEY_MANAGEMENT. Key management and key distribution between SEGFs shall comply to the Network Domain Security TS 133 210 [10]	FPT_ITA.1, FPT_ITC.1, FPT_ITI.2	TS 187 001 [3] clauses 4.6 and 5.3, ISO/IEC 15408-2 [13] clauses 14.3.2, 14.4.2, 14.5.2

c.1.1.15	R.SEGF_FIREWALLS. NGN security protocols shall work with commonly-used firewalls	FPT_RVM.1, FPT_SEP.3, FPT_SSP.2	TS 187 001 [3] clauses 4.8 and 5.3, ISO/IEC 15408-2 [13] clauses 14.10.2, 14.11.2, 14.12.2
c.1.1.16	R.SEGF_FIREWALLS_NAT/NATP. NGN security protocols shall work in environments with NAT/NATP	FPT_RVM.1, FPT_SEP.3, FPT_SSP.2, FPT_TDC.1	TS 187 001 [3] clauses 4.8 and 5.3, ISO/IEC 15408-2 [13] clauses 14.10.2, 14.11.2, 14.12.2, 14.14.2
c.1.1.17	R.SEGF_FILTERS. Filters to screen the IP packets to restrict/grant access to specific bearer streams shall be supported	FPT_ITA.1, FPT_ITC.1, FPT_ITI.2	TS 187 001 [3] clauses 4.8 and 5.3, ISO/IEC 15408-2 [13] clauses 14.3.2, 14.4.2, 14.5.2
c.1.2 TOE security assurance requirements			
c.1.2.1	Not applicable		
c.2 Environment security requirements (OPTIONAL) (named in the format RE.{key word(s) from textual description)			
c.2.1	RE.SEG B_IMPLEMENT_IPSEC_SA. Secure bi-directional communication between two SEGs using two IPsec Security Associations (one in each direction) – in network B	FDP_UCT.1, FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MSA.1(1), FMT_MSA.1(2), and FMT_MSA.2	TS 133 210 [10] clause 5.4, ISO/IEC 15408-2 [13] clauses 10.12.2, 10.13.2, 12.1.2 and 12.2.2
c.2.2	RE. SEG B_IMPLEMENT_ISAKMP_SA. Secure bi-directional communication between two SEGs using an ISAKMP Security Association – in network B	FDP_UCT.1, FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MSA.1(1), FMT_MSA.1(2), and FMT_MSA.2	TS 133 210 [10] clause 5.4, ISO/IEC 15408-2 [13] clauses 10.12.2, 10.13.2, 12.1.2 and 12.2.2

4.2.6 Application notes (OPTIONAL)

ISO/IEC 15408-1 [12] provides for optional application notes to be included in a PP. It is intended that this should include any additional information that might be considered useful to either or both of the implementor and the evaluator. This clause should be unnecessary if the base security standard has been fully and carefully specified.

d Application notes (OPTIONAL)
Not applicable

4.2.7 Rationale

ISO/IEC 15408-1 [12] requires that a PP provides a rationale, subdivided into security objectives rationale and security requirements rationale to explain in detail how the security objectives and the security requirements, respectively, address the threats identified in the TOE security environment. This rationale should be included in the Vulnerability Analysis.

E Rationale
Not applicable

4.3 NGN H.248 Deployment Partial PP

This clause illustrates the rationale used when building the PP for H.248 deployment using the guidance from ES 202 382 [6]. The closest identified target document is ES 283 002 [8].

4.3.1 PP Introduction

4.3.1.1 PP identification

A PP is required to provide enough labelling and descriptive information to enable it to be identified, catalogued, registered and cross referenced. The document number, version, date and full title of an ETSI standard are sufficient for this purpose and should be used.

Protection Profile					
Introduction					
Doc No.	ES 283 002	Version	v.1.1.1	Date	2005-08
Full Title	"Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Subsystem (PES); NGN Release 1: H.248 Profile for controlling Access and Residential Gateways" [8].				

4.3.1.2 PP overview

A PP should include a narrative summary as part of the Introduction. The purpose of this is to provide enough information that a potential user can make an informed decision on whether the PP is likely to be of interest. A fully specified Scope clause from an ETSI standard meets this requirement and should be used.

The existing scope from ES 283 002 [8] is quoted below:

QUOTE: *The present document defines a profile of the Gateway Control Protocol (H.248.1), for controlling access and residential gateways connecting analog lines and ISDN primary and basic access, in order to emulate PSTN/ISDN services over IP.*

The quoted scope statement gives a satisfactory summary of what H.248 deployment offers.

Overview	The target document defines a profile of the Gateway Control Protocol (H.248.1), for controlling access and residential gateways connecting analog lines and ISDN primary and basic access, in order to emulate PSTN/ISDN services over IP. This PP identifies security functions and assurances representative of the lowest common set of requirements that should be addressed by a useful H.248 implementation in NGN. A Target of Evaluation (TOE) compliant with this PP should meet the assurance requirements of Evaluation Assurance Level 4 (EAL4), seen as a guidance level.

4.3.2 Target Of Evaluation (TOE) description

NOTE 1: Throughout the present document, the term "Target Of Evaluation (TOE)" is used to identify any product which implements the technical requirements of the standard(s) associated with a particular PP.

The standard ISO/IEC 15408-1 [12] requires that a brief but clear description of the Target Of Evaluation (TOE) should be included in a PP. While not expressing the security requirements in detail, this should make the security aspects of the standard clear. If the standard includes a short clause entitled "General Description" (or something similar) early in the document, it is likely that this text will be adequate as the TOE description. In the event that such a clause does not exist it will need to be written for the PP and should include the following:

- identification of the type of product that is likely to implement the standard;

NOTE 2: In the context of the present document, the term "product" should be interpreted in its widest sense to include all types of communications equipment as well as services.

- general summary of the communications features specified in the standard or set of standards;
- brief overview of the security aspects specified in the standard.

The existing text of ES 283 002 [8] has descriptive clauses that provide information about the H.248 profile in NGN R1 (ES 283 002 [8] clauses 4.1, 4.2 and 5.2). The text is not quoted as the source document is referenced by the PP itself.

TOE Description

The figure illustrates the architecture assumed in the present document. The Media Gateway Controller (MGC) resides in a control subsystem and may be implemented as a stand-alone piece of equipment or as a component of a call server. Access to the IP network is provided to analog terminals, ISDN terminals, analog and ISDN PBXs through residential gateways or access gateways, which support one or more of the following reference points:

- Z reference point for analogue termination.
- T reference point for Primary rate Access.
- S/T reference point for Basic Rate Access.
- T* reference point for NMDS Access.

The reference model is shown below. The scope of the target document ES 283 002 [8] is the two marked interfaces (only).

No assumption is made about the structure of the control subsystem hosting the MGC functionality. In the context of the TISPAN NGN Architecture (see ES 282 002 [7]), the control subsystem is the PSTN/ISDN Emulation Subsystem (PES) according to ES 282 002 [7]. Within this subsystem, the AGCF plays the MGC role. The RGW and the AGW implement the R-MGF and A-MGF functional entities, respectively.
The use of IPsec (RFC 2401 [16]) to realize the operator security domain is outside the scope of the target document ES 283 002 [8].

4.3.3 TOE security environment

The TOE security environment should describe the security aspects of the environment in which the TOE is intended to be used. It is expected to include:

- security assumptions:
  - security aspects of the environment in which an implementation of a standard will be used;
  - the intended use of the implementation;
  - the physical, user and connection aspects of the environment in which an implementation will operate;
- threats:
  - all threats against which specific protection is required within either the implementation of a standard or its expected environment;
- organizational security policies:
  - any security policies or rules with which an implementation of a standard must comply.

The TOE security environment summarizes the results of a threat analysis of the communications system specified in the base standard. Threat analyses should be prepared following the process described in TISPAN documentation.

QUOTE: (clause 5.13, table 57 of ES 283 002 [8])
Supported security:

For the purpose of the present document the control protocols are considered to be inside the secured zone of a single operator as shown in figure 1. The specified H.248 security options should not be used, as these interfaces are considered to be within a secured zone.

In clause 7 of the present document protocols other than H.248 are specified and the security issues are dealt with here. No security measures, either IPsec or TLS, shall be used on the IUA interfaces since they too are considered to be within a secured zone. Finally no countermeasures shall be applied to the GRE interface carrying packet data.

Only the H.248 interface is considered in this PP (not the IUA and GRE interfaces).

No assumptions or specific threats are identified in the target document ES 283 002 [8]. In fact, the statement is that there is no need for security measures. For other scenarios, other security needs may be identified. See the quote below. The security for each such scenario must be investigated separately.

QUOTE: (clause 5.13, table 57 of ES 283 002 [8])
It is important to note that the context of this clause, and the recommendations in it, only applies to the case where the interfaces, H.248, IUA and GRE specified by the present document all fall within the secure zone shown in figure 1. In any other case a different risk may apply and appropriate countermeasures may be needed.

Taking the above into account for this PP, the TOE environment security requirements are addressed. In order to assure that the secured zone claim is valid. This is reflected in the PP table excerpts below.

a TOE Security Environment		
a.1 Assumptions (named in the format A.{key word(s) from textual description})		
a.1.1	A.SECURE_ZONE. The H.248 interface is within secured zone	ES 283 002 [8] clause 5.13
a.1.2	A.NO_SECURITY. The H.248 interface needs no security options	ES 283 002 [8] clause 5.13
a.1.3	A.RGW_ACCESS. Access and interface to RGW is secure	Indirectly stated in ES 283 002 [8] clause 5.13
a.1.4	A.AGW_ACCESS. Access and interface to AGW is secure	Indirectly stated in ES 283 002 [8] clause 5.13
a.2 Assets		
a.2.1		
a.3 Threat agents		
a.3.1	No specific TOE security environment threat agent has been identified in the target document or in other TISPAN NGN documentation	
a.4 Threats		
a.4.1	No specific TOE security environment threat has been identified in the target document or in other TISPAN NGN documentation	
a.5 Security policies (OPTIONAL) (named in the format P.{key word(s) from textual description})		
a.5.1	P.NO_SECURITY. No security options are to be used for H.248 in the scenario of the target document	ES 283 002 [8] clause 5.13
a.5.2	P.SECURITY. If H.248 is outside secure zone (such as in the case of multiple operators) then security options are to be considered	ES 283 002 [8] clause 5.13

4.3.4 Security objectives

A PP should contain a definition of the security objectives of both the TOE and its environment. These objectives are expected to cover the assumptions, threats and policies described in the TOE security environment (see clause 4.3.3). They should be expressed in broad terms rather than in detail and should be segregated into two distinct groups, thus:

- security objectives for the TOE:
  - it should be clear which aspects of the identified threats and policies are addressed by each objective;
  - if the base security standard specifies a protocol, it is likely that the TOE security objectives will be specified in the Stage 1 (or equivalent) specification.
- security objectives for the environment:
  - it should be clear 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 TOE security objectives;
  - 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. If this is the case, the objectives should be expressed in full in the PP.

No specific objectives have been identified for H.248 deployment security, see PP table excerpt below.

b Security Objectives		
b.1 Security objectives for the TOE		
b.1.1	No specific TOE security objective has been identified in the target document or in other TISPAN NGN documentation	
b.2 Security objectives for the environment		
b.2.1	No specific environment security objective has been identified in the target document or in other TISPAN NGN documentation	

4.3.5 IT security requirements

4.3.5.1 The relationship between security objectives and security requirements

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. As an example, the following statement is a security objective for a TOE:

- The TOE must identify and authenticate all users before granting access to the system.

One of the security requirements associated with this objective could be:

- A user shall be successfully identified and authenticated to the TOE by means of a user name and password before all other interactions between the TOE and that user.

NOTE: It would not be unusual for a single objective to be realized by the implementation of more than one requirement nor for a single requirement to partially implement more than one objective.

4.3.5.2 TOE security requirements

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

- TOE 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;
  - where possible, in indication of which of the functional components defined in ISO/IEC 15408-2 [13] the requirement represents.
- TOE security assurance requirements:
  - an indication of the Evaluation Assurance Level (EAL) 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 [14] which will apply to an implementation;
  - where necessary, a specification of any essential assurance requirements which are not included in ISO/IEC 15408-3 [14].

The specification of security requirements for the environment is optional and should only be included in the PP if security objectives for the environment are identified earlier in the PP (see clause 4.3.4). If requirements for the environment are included, they should be presented in the same way as functional requirements for the TOE.

No TOE security functional/assurance requirements have been identified for this PP, see PP table excerpt below. Two environment security requirements have been extracted indirectly from the target document.

c IT Security Requirements			
c.1 TOE security requirements			
c.1.1 TOE security functional requirements			
c.1.1.1	Not applicable		
c.1.2 TOE security assurance requirements			
c.1.2.1	Not applicable		
c.2 Environment security requirements (OPTIONAL) (named in the format RE.{key word(s) from textual description})			
c.2.1	RE.RGW_SECURED. Access and interface to the RGW have been secured	FPT_AMT.1, FPT_FLS.1, FPT_ITA.1, FPT_ITC.1, FPT_ITI,2, FPT_PHP.3, FPT_RCV.4, FPT_RPL.1, FPT_RVM.1, FPT_SEP.3, FPT_TDC.1, FPT_TRC.1, FPT_TST.1	Indirectly stated in ES 283 002 [8] clause 5.13, ISO/IEC 15408-2 [13] clauses 14.1.2, 14.2.2, 14.3.2, 14.4.2, 14.5.2, 14.7.2, 14.8.2, 14.9.2, 14.10.2, 14.11.2, 14.14.2, 14.15.2, 14.16.2
c.2.2	RE.AGW_SECURED. Access and interface to the AGW have been secured	FPT_AMT.1, FPT_FLS.1, FPT_ITA.1, FPT_ITC.1, FPT_ITI.2, FPT_PHP.3, FPT_RCV.4, FPT_RPL.1, FPT_RVM.1, FPT_SEP.3, FPT_TDC.1, FPT_TRC.1, FPT_TST.1	Indirectly stated in ES 283 002 [8] clause 5.13, ISO/IEC 15408-2 [13] clauses 14.1.2, 14.2.2, 14.3.2, 14.4.2, 14.5.2, 14.7.2, 14.8.2, 14.9.2, 14.10.2, 14.11.2, 14.14.2, 14.15.2, 14.16.2

4.3.6 Application notes (OPTIONAL)

ISO/IEC 15408-1 [12] provides for optional application notes to be included in a PP. It is intended that this should include any additional information that might be considered useful to either or both of the implementor and the evaluator. This clause should be unnecessary if the base security standard has been fully and carefully specified.

d Application notes (OPTIONAL)
This PP is valid for the (default) scenario stated in the target document only. Other scenarios as stated in the target document require other PPs.

4.3.7 Rationale

ISO/IEC 15408-1 [12] requires that a PP provides a rationale, subdivided into security objectives rationale and security requirements rationale to explain in detail how the security objectives and the security requirements, respectively, address the threats identified in the TOE security environment. This rationale should be included in the Vulnerability Analysis.

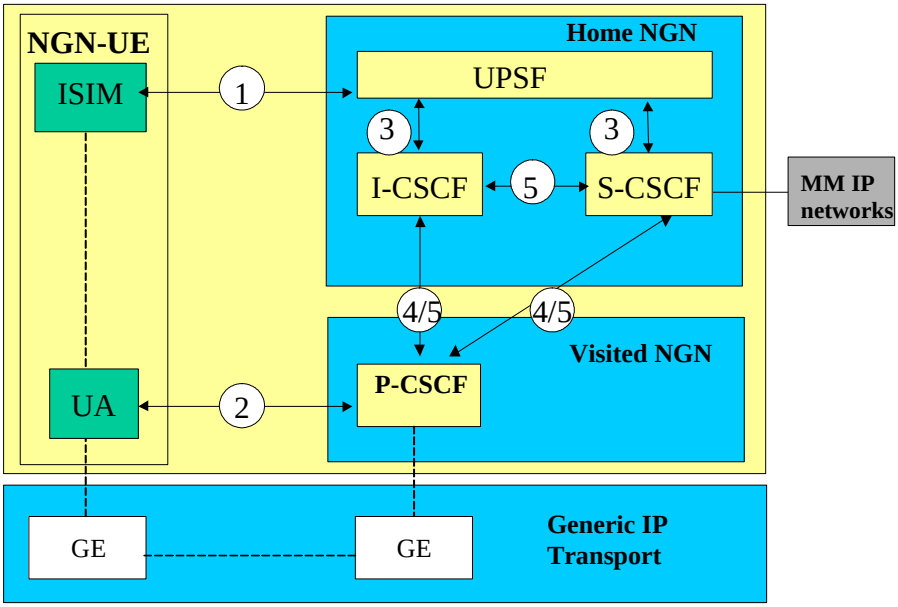
e Rationale
Not applicable

Annex A (informative): Partial Protection Profile (PP) for NGN-IMS Authentication

Protection Profile					
Introduction					
Doc No.	TS 133 203	Version	v.7	Date	2005-12
Full Title	"Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services (3GPP TS 33.203 version 7.0.0 Release 7)"				
Overview	The scope of the target document TS 133 203 [9] is to specify security features and mechanisms for secure access to the IM subsystem (IMS) in TISPAN. See normative annexes other than annex L in TS 133 203 [9]. This PP identifies security functions and assurances representative of the lowest common set of requirements that should be addressed by a useful NGN-IMS. A Target Of Evaluation (TOE) compliant with this PP should meet the assurance requirements of Evaluation Assurance Level 4 (EAL4), seen as a guidance level. The IMS in UMTS will support IP Multimedia applications such as video, audio and multimedia conferences. 3GPP has chosen SIP, Session Initiation Protocol, as the signalling protocol for creating and terminating Multimedia sessions. This specification only deals with how the SIP signalling is protected between the subscriber and the IMS, how the subscriber is authenticated and how the subscriber authenticates the IMS.				

TOE Description

In the PS domain, the service is not provided until a security association is established between the mobile equipment and the network. The IMS Security Architecture is shown in the figure.



IMS authentication keys and functions at the user side are stored on a UICC. The IMS authentication keys and functions are designed to be logically independent to the keys and functions used for PS domain authentication. However, this does not preclude common authentication keys and functions from being used for IMS and PS domain authentication.

There are five different security associations and different needs for security protection for IMS and they are numbered 1, 2, 3, 4 and 5 in the figure of which only association 1 is considered in this PP:

1. Provides mutual authentication. The HSS delegates the performance of subscriber authentication to the S-CSCF. However the HSS is responsible for generating keys and challenges. The long-term key in the ISIM and the HSS is associated with the IMPI. The subscriber will have one (network internal) user private identity (IMPI) and at least one external user public identity (IMPU).

Mutual authentication is required between the UE and the HN.

An independent IMS security mechanism provides additional protection against security breaches. For example, if the PS-Domain security is breached the IMS would continue to be protected by its own security mechanism. As indicated in the figure the P-CSCF may be located either in the Visited or the Home Network. The P-CSCF shall be co-located within the same network as the GGSN, which may reside in the VPLMN or HPLMN according to the APN and GGSN selection criteria.

a TOE Security Environment			
a.1 Assumptions			
a.1.1	No specific TOE security environment assumption has been identified in the target document or in other TISPAN NGN documentation		
a.2 Assets (named in the format AS.{key word(s) from textual description})			
a.2.1	AS.UICC_ISIM. UICC (with ISIM) equipment		TS 133 203 [9], TS 187 001 [3]
a.3 Threat agents			
a.3.1	No specific TOE security environment threat agent has been identified in the target document or in other TISPAN NGN documentation		
a.4 Threats (named in the format T.{key word(s) from textual description})			
a.4.1	T.INTERCEPT. Interception by: - Eavesdropping		TS 102 165-1 [1] clause 5.1.2
a.4.2	T.MANIPULATE. Manipulation by: - Masquerading ("spoofing"). - Loss or corruption of information. - Unauthorized access. - Forgery		TS 102 165-1 [1] clause 5.1.2
a.4.3	T.REPUDIATE_SEND. Repudiation of sending		TS 102 165-1 [1] clause 5.1.2
a.4.4	T.REPUDIATE_RECEIVE. Repudiation of receiving		TS 102 165-1 [1] clause 5.1.2
a.5 Security policies (OPTIONAL) (named in the format P.{key word(s) from textual description})			
a.5.1	P.SEPARATION. The TISPAN NGN network shall be logically and physically divided into security domains allowing for separation of application (e.g. IMS) and transport (e.g. ADSL or UMTS). Also different operators of similar networks (e.g. IMS) shall be able to operate their own security policies.		TS 187 001 [3] clause 4.1
a.5.2	P.MECHANISMS_CONFIGURABLE. Security mechanisms and other parameters beyond default security mechanisms shall be configurable. This shall be static for NNI interface and may be negotiated for UNI interfaces. The security mechanism negotiation shall have a certain minimum level to be identified by the security domain; e.g. avoid bidding-down attacks. Users shall be able to reject communications that do not conform to their minimum security policy.		TS 187 001 [3] clause 4.1
a.5.3	P.MECHANISMS_PARTITIONED. The security mechanisms shall be partitioned such that the functions of authentication, data integrity, replay detection, and confidentiality may be implemented and selected independently of each other, insofar as this makes sense.		TS 187 001 [3] clause 4.1
b Security Objectives			
b.1 Security objectives for the TOE			
b.1.1	No specific TOE security objective has been identified in the target document or in other TISPAN NGN documentation		
b.2 Security objectives for the environment			
b.2.1	No specific environment security objective has been identified in the target document or in other TISPAN NGN documentation		
c IT Security Requirements c.1 TOE security requirements			
c.1.1 TOE security functional requirements (named in the format R.{key word(s) from textual description})			
c.1.1.1	R.LEGACY. NGN R1 IMS authentication shall support early deployment scenarios (with support for legacy equipments).	FIA_UAU.3	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2
c.1.1.2	R.INDEPENDENT. In non-early deployment scenarios, IMS authentication shall be independent from access authentication.	FIA_UAU.3	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2
c.1.1.3	R.ISIM_AUTHENTICATION. ISIM based Authentication between the IMS-subscriber and the network shall comply to the authentication part of Access Security for IP-based services TS 133 203 [9].	FIA_UAU.4	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2
c.1.1.4	R.ISIM_REAUTHENTICATION. ISIM based Re-authentication of an IMS-subscriber shall comply to the authentication part of Access Security for IP-based services TS 133 203 [9].	FIA_UAU.6	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2
c.1.1.5	R.ISIM_COMPLIANCE. ISIM based Re-authentication of an IMS-subscriber shall comply to the authentication part of Access Security for IP-based services TS 133 203 [9].	FIA_UAU.6	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2

c.1.1.6	R.SIP. User Authentication to the NGN IMS using SIP Digest mechanisms shall be supported as an early deployment scenario.	FIA_UAU.4	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2
c.1.1.7	R.SIP_AND_ISIM. Where both Digest and ISIM solutions are deployed by an NGN IMS operator, that operator shall determine the authentication mechanism (SIP Digest or ISIM-based) on a per-user basis. The authentication mechanism shall be enforced according to both the subscription information in the user's service profile and the specific policies of the NGN IMS operator.	FIA_UAU.4	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2
c.1.1.8	R.PASSWORDS. Transmitted passwords shall be sufficiently protected; e.g. by encryption or other techniques.	FDP_DAU.1, FIA_UAU.3	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clauses 10.3.2 and 11.4.2
c.1.1.9	R.EARLY_DEPLOYMENT. For the special early deployment scenarios, where IMS authentication is linked to access authentication, it shall be possible to gain access to IMS services after an authentication procedure. This authentication provides simultaneous access to the access network and IMS services.	FIA_UAU.4	TS 187 001 [3] clause 4.2, ISO/IEC 15408-2 [13] clause 11.4.2
c.1.2 TOE security assurance requirements			
c.1.2.1	Not applicable		
c.2 Environment security requirements (OPTIONAL)			
c.2.1	Not applicable		
d Application notes (OPTIONAL)			
Not applicable			
e Rationale			
Not applicable			

Annex B (informative): Partial Protection Profile (PP) for NGN-NDS Source Authentication

Protection Profile					
Introduction					
Doc No.	TS 133 210	Version	v.7	Date	2005-12
Full Title	"Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 version 7.0.0 Release 7)".				
Overview	The target document defines the security architecture for network domain IP based control planes, which shall be applied to NDS/IP-networks (i.e. 3GPP and fixed broadband networks). The scope of network domain control plane security is to cover the control signalling on selected interfaces between network elements of NDS/IP networks. This PP identifies security functions and assurances representative of the lowest common set of requirements that should be addressed by a useful NGN-NDS. A Target of Evaluation (TOE) compliant with this PP should meet the assurance requirements of Evaluation Assurance Level 4 (EAL4), seen as a guidance level. The scope of the target document TS 133 210 [10] is to outline the basic principles for the network domain security architecture. A central concept introduced in the target document is the notion of a security domain. The security domains are networks that are managed by a single administrative authority. Within a security domain the same level of security and usage of security services will be typical. Typically, a network operated by a single operator will constitute one security domain although an operator may at will subsection its network into separate sub-networks.				

TOE Description

The network domain control plane of an NDS/IP network is sectioned into security domains which typically coincide with operator borders. The border between the security domains is protected by Security Gateways (SEGs). The SEGs are responsible for enforcing the security policies towards other SEGs and for the interworking of networks. SEGs are designed to handle communication over the Za interface. The security may include filtering policies and firewall functionality not specified in the target document TS 133 210 [10].

This PP addresses communication between a Securityy Gateway (SEG) in one NDS and another SEG in a neighbouring NDS. The setup is depicted in the figure (based upon TS 133 210 [10] clause 5).

In NDS the IPsec security protocol shall always be ESP (TS 133 210 [10] clause 5.1). In NDS it is mandated that integrity protection/message authentication, together with anti-replay protection, shall always be used.

The security services provided by NDS/IP are (TS 133 210 [10] clause 5.1):

- Data integrity.
- Data origin authentication.
- Anti-replay protection.
- Confidentiality (OPTIONAL).

There is limited protection against traffic flow analysis when confidentiality is applied. The PP covers the use of the data origin authentication service only.

For native IP-based protocols, security is provided at the network layer. The security protocols used at the network layer are the IETF defined IPsec security protocols as specified in RFC 2401 [16]. The network domain security of an NDS/IP network does not extend to the user plane. Consequently, the security domains and the associated SEGs do not encompass the user plane Gi interface towards other, possibly external, IP networks.

A chained-tunnel/hub-and-spoke approach is used. This facilitates hop-by-hop based security protection. All NDS/IP traffic passes through a SEG before entering or leaving the security domain. SEGs are physically secured and offer secure storage of long-term keys used for IKE authentication.

a TOE Security Environment		
a.1 Assumptions (named in the format A.{key word(s) from textual description})		
a.1.1	A.SECURITY_DOMAINS. The network domain control plane of an NDS/IP network is physically and logically sectioned into security domains. Typically these coincide with operator borders.	TS 133 210 [10] clauses 4.3 and 4.4.1
a.1.2	A.BORDER_PROTECTION. The border between security domains is protected by Security Gateways (SEGs).	TS 133 210 [10] clauses 4.3 and 4.5
a.1.3	A.SEG_ENFORCING. A SEG is responsible for enforcing the security policy of a security domain towards another SEG in a destination security domain, and for the interworking between these networks. The security may include filtering policies and firewall functionality.	TS 133 210 [10] clauses 4.3, 4.5 and 5.6.1
a.1.4	A.SEG_NUMBER. A security domain can have one or more SEGs, depending on the need to differentiate between the externally reachable destinations, the need to balance the traffic load, to avoid single points of failure, or for performance reasons.	TS 133 210 [10] clauses 4.3, 4.5
a.1.5	A.SEG_REACHABILITY. A SEG may be defined for interaction towards all reachable security domains, or it may be defined for only a subset of the reachable destinations. A SEG handles NDS/IP traffic in or out of a security domain, towards a well-defined set of other, reachable IP security domains.	TS 133 210 [10] clauses 4.3, 4.5 and 5.6.1
a.1.6	A.USER_PLANE. The network domain security of an NDS/IP network does not extend to the user plane, the consequence being that the security domains and the associated SEGs towards other domains do not encompass the user interface Gi interface towards other, possibly external, IP networks.	TS 133 210 [10] clause 4.3
a.1.7	A.HOP_BY_HOP. A chained-tunnels or hub-and-spoke approach is used to facilitate hop-by-hop based security protection.	TS 133 210 [10] clauses 4.3 and 5.6.1
a.1.8	A.SEG_SECURES_NATIVE_IP. A SEG secures native IP based protocols.	TS 133 210 [10] clause 4.5
a.1.9	A.SEG_OVER_ZA_IF. A SEG handles communication over Za interface, located between SEGs in different IP security domains.	TS 133 210 [10] clauses 4.5 and 5.6.2
a.1.10	A.IPSEC_SA. IPsec offers a set of security services, which is determined by the negotiated IPsec Security Associations (IPsec SAs). The IPsec SAs define which security protocol to be used, the mode and the end points of the SA.	TS 133 210 [10] clause 5.1
a.1.11	A.IKE. For NDS/IP networks the key management and distribution between SEGs is handled by the protocol Internet Key Exchange (IKE).	TS 133 210 [10] clause 5.2, RFC 2407 [17], RFC 2408 [18], RFC 2409 [19]
a.1.12	A.TUNNEL_MODE_SUPPORT. NDS/IP only requires support for tunnel mode IPsec SAs.	TS 133 210 [10] clause 5.2
a.1.13	A.ESP_SA_SUPPORT. NDS/IP only requires support for ESP SAs.	TS 133 210 [10] clause 5.2
a.1.14	A.NEGOTIATE BUNDLES. There is no need to be able to negotiate IPsec SA bundles since a single ESP SA is sufficient to set up to protect traffic between nodes.	TS 133 210 [10] clause 5.2
a.1.15	A.SPD_INSTRUMENT. The Security Policy Database (SPD) is a policy instrument to decide which security services are to be offered and in what fashion.	TS 133 210 [10] clause 5.2.1
a.1.16	A.SPD_ROLE. The SPD plays a central role when defining security policies, both within the internal security domain and towards external security domains. The security policy towards external security domains is subject to roaming agreements.	TS 133 210 [10] clause 5.2.1
a.1.17	A.SAD_PARAMETERS. The Security Association Database (SAD) contains parameters that are associated with the active security associations. Every SA has an entry in the SAD.	TS 133 210 [10] clause 5.2.2
a.1.18	A.SAD_OUTBOUND. For outbound processing, a lookup in the SPD will point to an entry in the SAD. If an SPD entry does not point to an SA that is appropriate, an SA is automatically created.	TS 133 210 [10] clause 5.2.2
a.1.19	A.RANDOM_DATA. NDS/IP contains element(s) that can generate random data (for IV).	TS 133 210 [10] clause 5.3.5, RFC 1750 [15]
a.2 Assets (named in the format AS.{key word(s) from textual description})		
a.2.1	AS.NDS_PHYSICAL. Security domain, NDS.	TS 133 210 [10] clause 4.4.1
a.2.2	AS.NDS_IF_PHYSICAL. Security domain interface, NDS IF.	TS 133 210 [10] clause 4.4.1
a.2.3	AS.SEG. SEG (Security Gateway), in domain A	TS 133 210 [10] clause 4.5

a.2.4	AS.SPD_PHYSICAL. Security Policy Database (SPD) platform	TS 133 210 [10] clause 5.2.1
a.2.5	AS.SAD_PHYSICAL. Security Association Database (SAD) platform	TS 133 210 [10] clause 5.2.2
a.2.6	AS.SPD_OUTBOUND. Security Policy Database (SPD) outbound entries	TS 133 210 [10] clause 5.2.1
a.2.7	AS.SPD_INBOUND. Security Policy Database (SPD) inbound entries	TS 133 210 [10] clause 5.2.1
a.2.8	AS.SAD. Security Association Database (SAD) entries	TS 133 210 [10] clause 5.2.2
a.2.9	AS.NDS_LOGICAL. Security domain, NDS	TS 133 210 [10] clause 4.4.1
a.2.10	AS.NDS_IF_LOGICAL. Security domain interface, NDS IF	TS 133 210 [10] clause 4.5
a.2.11	AS.IPSEC. TBD/Logical/Procedure/TBD: IPsec	TS 133 210 [10] clause 5.2
a.2.12	AS.IPSEC_SA_1. TBD/Logical/Procedure/TBD: IPsec Security Association (SA) 1	TS 133 210 [10] clause 5.2
a.2.13	AS.IPSEC_SA_2. TBD/Logical/Procedure/TBD: IPsec Security Association (SA) 2	TS 133 210 [10] clause 5.2
a.2.14	AS.IKE. TBD/Logical/Procedure/TBD : IKE	TS 133 210 [10] clause 5.2
a.2.15	AS.ISAKMP_SA. TBD/Logical/Procedure/TBD: ISAKMP Security Association (SA) with pre-shared keys	TS 133 210 [10] clause 5.2
a.3 Threat agents		
a.3.1	No specific TOE security environment threat agent has been identified in the target document or in other TISPAN NGN documentation	
a.4 Threats (named in the format T.{key word(s) from textual description})		
a.4.1	T.INTERCEPT. Interception by eavesdropping	TS 102 165-1 [1] clause 5.1.2
a.4.2	T.MANIPULATE. Manipulation by: - Masquerading ("spoofing"). - Loss or corruption of information. - Unauthorized access. - Forgery	TS 102 165-1 [1] clause 5.1.2
a.4.3	T.REPUDIATE_SEND. Repudiation of sending	TS 102 165-1 [1] clause 5.1.2
a.4.4	T.REPUDIATE_RECEIVE. Repudiation of receiving	TS 102 165-1 [1] clause 5.1.2
a.5 Security policies (OPTIONAL) (named in the format P.{key word(s) from textual description})		
a.5.1	P.POLICY_DATABASE: Security Policy Database (SPD) is a policy instrument to decide which services are to be offered and in what fashion	TS 133 210 [10] clause 5.2.1
a.5.2	P.IN_OUTBOUND: SPD shall be consulted during processing of both inbound and outbound traffic. Includes traffic not protected by IPsec. SPD must have unique entries for inbound and outbound traffic so that SPD can discriminate among traffic protected by IPsec, bypassing IPsec, or discarded by IPsec.	TS 133 210 [10] clause 5.2.1
a.5.3	P.GRANULARITY: Policy control granularity afforded by NDS/IP is determined by degree of control with respect to ESP Security Association between NEs and SEGs. Normal mode of operation is that only one ESP SA is used between any two NEs or SEGs. Therefore the security policy is identical to all secured traffic passing between NEs.	TS 133 210 [10] clause 5.5
a.5.4	P.INTRA_DOMAIN: Security domains should have the same security policy in force for all traffic within the security domain	TS 133 210 [10] clause 5.5
a.5.5	P.INTER_DOMAIN: The inter-security domain policy is determined by roaming agreements when security domains belong to different operators	TS 133 210 [10] clause 5.5, TS 187 001 [3] clause 4.1
a.5.6	P.IPSEC_SEG: IPsec security policy enforcement for inter-security domain communication is a matter for SEGs of communicating security domains	TS 133 210 [10] clause 5.5
b Security Objectives		
b.1 Security objectives for the TOE (named in the format O.{key word(s) from textual description})		
b.1.1	O.BI-DIRECTIONAL: To secure bi-directional communication between two SEGs	TS 133 210 [10] clause 5.2
b.2 Security objectives for the environment (named in the format OE.{key word(s) from textual description})		
b.2.1	OE.SEG B_BI-DIRECTIONAL: To secure bi-directional communication between two SEGs – in other network	TS 133 210 [10] clause 5.2

c IT Security Requirements			
c.1 TOE security requirements			
c.1.1 TOE security functional requirements (named in the format R.{key word(s) from textual description})			
c.1.1.1	R.IMPLEMENT_IPSEC_SA. Secure bi-directional communication between two SEGs shall be established using two IPsec Security Associations (one in each direction).	FDP_UCT.1 FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FMT_MSA.1 (1), FMT_MSA.1 (2) and FMT_MSA.2	TS 133 210 [10] clause 5.4, ISO/IEC 15408-2 [13] clauses 10.12.2, 10.13.2, 12.1.2 and 12.2.2
c.1.1.2	R.IMPLEMENT_ISAKMP_SA. Secure bi-directional communication between two SEGs shall be established using an ISAKMP Security Association.	FDP_UCT.1, FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FMT_MSA.1 (1), FMT_MSA.1 (2) and FMT_MSA.2	TS 133 210 [10] clause 5.4, ISO/IEC 15408-2 [13] clauses 10.12.2, 10.13.2, 12.1.2 and 12.2.2
c.1.1.3	R.ESP_3DES. ESP 3DES (CBC) encryption transform shall be supported.	FDP_UCT.1, FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FMT_MOF.1 (1), FMT_MOF.1 (2), FMT_MOF.1 (3), FMT_MSA.1 (1), FMT_MSA.1 (2) and FMT_MSA.2	TS 133 210 [10] clause 5.1, 5.3.1, 5.3.3 and 5.4, ISO/IEC 15408-2 [13] clauses 10.12.2, 10.13.2, 12.1.2 and 12.2.2
c.1.1.4	R.SPD. The SPD shall be consulted during processing of both inbound and outbound traffic.	FDP_DAU.1, FDP_DAU.2, FDP_SDI.1, FDP_SDI.2, FDP_UCT.1, FDP_UIT.1, FDP_UIT.2 and FDP_UIT.3	TS 133 210 [10] clause 5.2.1, ISO/IEC 15408-2 [13] clauses 10.3.2, 10.11.2, 10.12.2 and 10.13.2
c.1.1.5	R.SAD. An SA shall be automatically created if and SPD entry does not point to an SA that is appropriate for the packet.	FDP_DAU.1, FDP_DAU.2, FDP_SDI.1, FDP_SDI.2, FDP_UCT.1, FDP_UIT.1, FDP_UIT.2 and FDP_UIT.3	TS 133 210 [10] clause 5.2.2, ISO/IEC 15408-2 [13] clauses 10.3.2, 10.11.2, 10.12.2 and 10.13.2
c.1.1.6	R.AES_CBC. AES CBC cipher algorithm shall be supported.	FDP_UCT.1, FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FMT_MOF.1 (1), FMT_MOF.1 (2), FMT_MOF.1 (3), FMT_MSA.1 (1), FMT_MSA.1 (2) and FMT_MSA.2	TS 133 210 [10] clauses 5.3.3 and 5.4, ISO/IEC 15408-2 [13] clauses 10.12.2, 10.13.2, 12.1.2 and 12.2.2
c.1.1.7	R.ESP_AUTHENTICATION. ESP_HMAC_SHA-1 authentication transform shall be supported.	FDP_UCT.1, FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FMT_MOF.1 (1), FMT_MOF.1 (2), FMT_MOF.1 (3), FMT_MSA.1 (1), FMT_MSA.1 (2) and FMT_MSA.2	TS 133 210 [10] clauses 5.2, 5.3.4 and 5.4, ISO/IEC 15408-2 [13] clauses 10.12.2, 10.13.2, 12.1.2 and 12.2.2

c.1.1.8	R.IV_RANDOM. Random data generation capability, for IV shall be supported.	FDP_UCT.1, FDP_UIT.2 and FDP_UIT.3	TS 133 210 [10] clause 5.3.5, RFC 1750 [15], ISO/IEC 15408-2 [13] clauses 10.12.2 and 10.13.2
c.1.1.9	R.ENFORCE_POLICIES. The security gateway functions (SEGF) shall be responsible for enforcing security policies for the interworking between networks.	FPT_FLS.1, FPT_ITA.1, FPT_ITC.1, FPT_ITI.1, FPT_PHP.3, FPT_RCV.4, FPT_RPL.1, FPT_RVM.1, FPT_SEP.3, FPT_SSP.2, FPT_TDC.1, FPT_TST.1	TS 133 210 [10] clause 4.5, TS 187 001 [3] clause 4.1, ISO/IEC 15408-2 [13] clauses 14.2.2, 14.3.2, 14.4.2, 14.5.2, 14.7.2, 14.8.2, 14.9.2, 14.10.2, 14.11.2, 14.12.2, 14.14.2 and 14.16.2
c.1.1.10	R.SECURE_STORAGE. SEGFs are responsible for security sensitive operations and shall offer capabilities for secure storage of long-term keys used for IKE authentication.	FPT_FLS.1, FPT_ITA.1, FPT_PHP.3, FPT_RCV.4	TS 133 210 [10] clause 4.5, TS 187 001 [3] clause 4.1, ISO/IEC 15408-2 [13] clauses 14.2.2, 14.3.2, 14.7.2 and 14.8.2
c.1.1.11	R.NDS. Network Domain Security (NDS) shall be provided at the network layer and comply to TS 133 210 [10].	FPT_FLS.1, FPT_ITA.1, FPT_ITC.1, FPT_ITI.1, FPT_RPL.1, FPT_RVM.1, FPT_SEP.3, FPT_SSP.2, FPT_TDC.1, FPT_TST.1	TS 187 001 [3] clause 4.4.1, ISO/IEC 15408-2 [13] clauses 14.2.2, 14.3.2, 14.4.2, 14.5.2, 14.7.2, 14.10.2, 14.11.2, 14.12.2, 14.14.2 and 14.16.2
c.1.1.12	R.SEGF. All NDS/IP traffic shall pass through a SEG, Security Gateway (SEGF, Security Gateway Function) before entering or leaving the security domain.	FPT_RVM.1	TS 133 210 [10] clauses 4.3 and 4.5, TS 187 001 [3] clause 4.4.1, ISO/IEC 15408-2 [13] clause 14.10.2
c.1.1.13	R.ZA_INTERFACE. IMS operators shall operate NDS/IP Za interface between SEGFs according to TS 133 210 [10].	FPT_ITA.1, FPT_ITC.1, FPT_ITI.2	TS 187 001 [3] clause 4.4.1, ISO/IEC 15408-2 [13] clauses 14.3.2, 14.4.2 and 14.5.2
c.1.1.14	R.KEY_MANAGEMENT. Key management and key distribution between SEGFs shall comply to the Network Domain Security TS 133 210 [10].	FPT_ITA.1, FPT_ITC.1, FPT_ITI.2	TS 187 001 [3] clauses 4.6 and 5.3, ISO/IEC 15408-2 [13] clauses 14.3.2, 14.4.2 and 14.5.2
c.1.1.15	R.SEGF_FIREWALLS. NGN security protocols shall work with commonly-used firewalls.	FPT_RVM.1, FPT_SEP.3, FPT_SSP.2	TS 187 001 [3] clause 4.8 and 5.3, ISO/IEC 15408-2 [13] clauses 14.10.2, 14.11.2 and 14.12.2
c.1.1.16	R.SEGF_FIREWALLS_NAT/NATP. NGN security protocols shall work in environments with NAT/NATP.	FPT_RVM.1, FPT_SEP.3, FPT_SSP.2, FPT_TDC.1	TS 187 001 [3] clauses 4.8 and 5.3, ISO/IEC 15408-2 [13] clauses 14.10.2, 14.11.2, 14.12.2 and 14.14.2
c.1.1.17	R.SEGF_FILTERS. Filters to screen the IP packets to restrict/grant access to specific bearer streams shall be supported.	FPT_ITA.1, FPT_ITC.1, FPT_ITI.2	TS 187 001 [3] clauses 4.8 and 5.3, ISO/IEC 15408-2 [13] clauses 14.3.2, 14.4.2 and 14.5.2

c.1.2 TOE security assurance requirements			
c.1.2.1	Not applicable		
c.2 Environment security requirements (OPTIONAL)			
c.2.1	Not applicable		
d Application notes (OPTIONAL)			
Not applicable			
e Rationale			
Not applicable			

Annex C (informative): Partial Protection Profile (PP) for NGN H.248 Deployment

<table>
<tr><th colspan="6">Protection Profile</th></tr>
<tr><td colspan="6">Introduction</td></tr>
<tr><td>Doc No.</td><td>ES 283 002</td><td>Version</td><td>v.1.1.1</td><td>Date</td><td>2005-08</td></tr>
<tr><td>Full Title</td><td colspan="5">"Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Subsystem (PES); NGN Release 1; H.248 Profile for controlling Access and Residential Gateways".</td></tr>
<tr><td>Overview</td><td colspan="5">The target document defines a profile of the Gateway Control Protocol (H.248.1), for controlling access and residential gateways connecting analog lines and ISDN primary and basic access, in order to emulate PSTN/ISDN services over IP.
This PP identifies security functions and assurances representative of the lowest common set of requirements that should be addressed by a useful H.248 implementation in NGN. A Target of Evaluation (TOE) compliant with this PP should meet the assurance requirements of Evaluation Assurance Level 4 (EAL4), seen as a guidance level.</td></tr>
<tr><td colspan="6">TOE Description</td></tr>
<tr><td colspan="6">The figure illustrates the architecture assumed in the present document. The Media Gateway Controller (MGC) resides in a control subsystem and may be implemented as a stand-alone piece of equipment or as a component of a call server. Access to the IP network is provided to analog terminals, ISDN terminals, analog and ISDN PBXs through residential gateways or access gateways, which support one or more of the following reference points:

1) Z reference point for analogue termination.

2) T reference point for Primary rate Access.

3) S/T reference point for Basic Rate Access.

4) T* reference point for NMDS Access.

The reference model is shown below. The scope of the target document ES 283 002 [8] is the two marked interfaces (only).

No assumption is made about the structure of the control subsystem hosting the MGC functionality. In the context of the TISPAN NGN Architecture (see ES 282 002 [7]), the control subsystem is the PSTN/ISDN Emulation Subsystem (PES) according to ES 282 002 [7]. Within this subsystem, the AGCF plays the MGC role. The RGW and the AGW implement the R-MGF and A-MGF functional entities, respectively.

The use of IPsec (RFC 2401 [16]) to realize the operator security domain is outside the scope of the target document ES 283 002 [8].</td></tr>
</table>

Protection Profile		
a TOE Security Environment		
a.1 Assumptions (named in the format A.{key word(s) from textual description})		
a.1.1	A.SECURE_ZONE. The H.248 interface is within secured zone	ES 283 002 [8] clause 5.13
a.1.2	A.NO_SECURITY. The H.248 interface needs no security options	ES 283 002 [8] clause 5.13
a.1.3	A.RGW_ACCESS. Access and interface to RGW is secure	Indirectly stated in ES 283 002 [8] clause 5.13
a.1.4	A.AGW_ACCESS. Access and interface to AGW is secure	Indirectly stated in ES 283 002 [8] clause 5.13
a.2 Assets (named in the format AS.{key word(s) from textual description})		
a.2.1	AS.SECURE_ZONE. Secured zone not requiring H.248 security options	Indirectly stated in ES 283 002 [8] clause 5.13
a.3 Threat agents		
a.3.1	No specific TOE security environment threat agent has been identified in the target document or in other TISPAN NGN documentation	
a.4 Threats		
a.4.1	No specific TOE security environment threat has been identified in the target document or in other TISPAN NGN documentation	
a.5 Security policies (OPTIONAL) (named in the format P.{key word(s) from textual description})		
a.5.1	P.NO_SECURITY. No security options are to be used for H.248 in the scenario of the target document	ES 283 002 [8] clause 5.13
a.5.2	P.SECURITY. If H.248 is outside secure zone (such as in the case of multiple operators) then security options are to be considered	ES 283 002 [8] clause 5.13
b Security Objectives		
b.1 Security objectives for the TOE		
b.1.1	No specific TOE security objective has been identified in the target document or in other TISPAN NGN documentation	
b.2 Security objectives for the environment		
b.2.1	No specific environment security objective has been identified in the target document or in other TISPAN NGN documentation	

Protection Profile			
c IT Security Requirements			
c.1 TOE security requirements			
c.1.1 TOE security functional requirements			
c.1.1.1	Not applicable		
c.1.2 TOE security assurance requirements			
c.1.2.1	Not applicable		
c.2 Environment security requirements (OPTIONAL) (named in the format RE.{key word(s) from textual description})			
c.2.1	RE.RGW_SECURED. Access and interface to the RGW have been secured	FPT_AMT.1, FPT_FLS.1, FPT_ITA.1, FPT_ITC.1, FPT_ITI,2, FPT_PHP.3, FPT_RCV.4, FPT_RPL.1, FPT_RVM.1, FPT_SEP.3, FPT_TDC.1, FPT_TRC.1, FPT_TST.1	Indirectly stated in ES 283 002 [8] clause 5.13, ISO/IEC 15408-2 [13] clauses 14.1.2, 14.2.2, 14.3.2, 14.4.2, 14.5.2, 14.7.2, 14.8.2, 14.9.2, 14.10.2, 14.11.2, 14.14.2, 14.15.2 and 14.16.2
c.2.2	RE.AGW_SECURED. Access and interface to the AGW have been secured	FPT_AMT.1, FPT_FLS.1, FPT_ITA.1, FPT_ITC.1, FPT_ITI.2, FPT_PHP.3, FPT_RCV.4, FPT_RPL.1, FPT_RVM.1, FPT_SEP.3, FPT_TDC.1, FPT_TRC.1, FPT_TST.1	Indirectly stated in ES 283 002 [8] clause 5.13, ISO/IEC 15408-2 [13] clauses 14.1.2, 14.2.2, 14.3.2, 14.4.2, 14.5.2, 14.7.2, 14.8.2, 14.9.2, 14.10.2, 14.11.2, 14.14.2, 14.15.2 and 14.16.2
d Application notes (OPTIONAL)			
This PP is valid for the (default) scenario stated in the target document only. Other scenarios as stated in the target document require other PPs.			
e Rationale			
Not applicable			

Annex D (informative): Bibliography

- ETSI TS 100 929: "Digital cellular telecommunications system (Phase 2+); Security-related network functions (3GPP TS 03.20)".
- ETSI TS 100 920: "Digital cellular telecommunications system (Phase 2+); Security aspects (3GPP TS 02.09)".
- ETSI TS 100 614: "Digital cellular telecommunications system (Phase 2+) (GSM); Security management (GSM 12.03)".
- ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- ETSI TS 101 303: "Telecommunications and Internet Protocol Harmonization Over Networks (TISPAN) Release 4; Service Independent Requirements Definition; Service and Network Management Framework; Overview and Introduction".
- ETSI TS 101 882-2: "Telecommunications and Internet Protocol Harmonization Over Networks (TISPAN) Release 4; Protocol Framework Definition; part 2; Registration and Service Attachment service meta-protocol definition".
- ITU-T Recommendation H.225.0 (Version 2): "Call Signalling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems".
- ITU-T Recommendation H.245 (Version 3): "Control Protocol for Multimedia Communication".
- ITU-T Recommendation H.323 (Version 3): "Packet Based Multimedia Communication Systems".
- ITU-T Recommendation H.323 Annex F: "Simple Endpoint Types".
- ITU-T Recommendation H.323 Annex J: "Security for H.323 Annex F".
- ITU-T Recommendation H.235 (Version 2): "Security and Encryption for H Series (H.323 and other H.245 based) multimedia terminals".
- IETF RFC 3261: "Session Initiation Protocol".
- ETSI TS 121 133: "Universal Mobile Telecommunications System (UMTS); 3G security; Security threats and requirements (3GPP TS 21.133)".
- ETSI EG 202 549: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Design Guide; Application of security countermeasures to service capabilities".

History

Document history		
V1.1.1	November 2006	Publication