ETSI TR 187 019 V3.1.1 (2011-02)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Feasibility Study of Security of NGN Interconnection at the NNI for Release 3; Interconnection security

Reference

DTR/TISPAN-07043-NGN-R3

Keywords

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

1 Scope

The present document addresses issues related to interoperator NNI interface interconnection. Security issues on NNI interconnections between the different subsystems of the NGN will also be addressed. The present document will identify the impact on 3GPP and TISPAN specifications.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) 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.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[i.2] ETSI TS 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

[i.3] ETSI TS 187 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 2 Lawful Interception; Stage 1 and Stage 2 definition".

[i.4] ETSI TR 187 009: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study of prevention of unsolicited communication in the NGN".

[i.5] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)".

[i.6] ETSI ES 282 001: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[i.7] ETSI TS 181 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability Requirements".

[i.8] ETSI TR 184 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Infrastructure ENUM Options for a TISPAN IPX".

[i.9] IETF RFC 2246 (1999): "Transport Layer Security version 1.0".

[i.10] ETSI TS 133 203: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Access security for IP-based services (3GPP TS 33.203)".".

[i.11] ETSI TS 133 310: "Universal Mobile Telecommunications System (UMTS); LTE; Network Domain Security (NDS); Authentication Framework (AF) (3GPP TS 33.310)".".

[i.12] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229)".

[i.13] ETSI TR 187 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NAT traversal feasibility study report".

[i.14] ETSI TR 187 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study on Media Security in TISPAN NGN".

[i.15] ETSI TS 133 328: "Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS) media plane security (3GPP TS 33.328)".".

[i.16] ETSI TR 187 015: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Specifications for PUC (Prevention of Unsolicited Communication) in the NGN".

[i.17] ETSI TS 133 220: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (3GPP TS 33.220)".

[i.18] IETF RFC 3261: "SIP: Session Initiation Protocol".

3 Abbreviations

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

3G	3rd Generation
3GPP	3rd Generation Partnership Project
AS	Application Server
CoIx	Connectivity oriented Interconnection
CSCF	Call Session Control Function
DoS	Denial-of-Service
I-BGF	Interconnect Border Gateway Function
ID	IDentity
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSEC	Internet Protocol Security
IT	Information Technology
IWF	Inter-Working Function
NAF	operator controlled Network Application Function
NAPT	Network Address and Port Translations
NASS	Network Access SubSystem
NAT	Network Address Translation
NDS	Network Domain Security
NGN	Next Generation Network
NNI	Network to Network Interface
PES	PSTN/ISDN Emulation Subsystem
RACS	Resource Admission Control Subsystem
SBC	Session Border Controller
SEGF	SEcurity Gateway Functions
SIP	Session Initiation Protocol
SoIx	Service oriented Interconnection
THIG	Topology-Hiding Inter-network Gateway

TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
TLS	Transport Layer Security
TS	Technical Specification
UMTS	Universal Mobile Telecommunication System
UNI	User to Network Interface

4 Main interconnection use cases

This clause contains the main interconnection use cases to take into consideration for the security analysis of the present document. The scope of the clause is to list the already defined interconnection scenarios, without defining new ones.

4.1 TISPAN Interconnection scenarios

The ES 282 001 NGN Functional Architecture [i.6] describes all the NGN interconnection scenarios relevant for the TISPAN context. The NNI interconnection scenarios have been divided taking into account the layer involved. Currently the following categories have been defined:

- Interconnection at the transport layer:
    - Interconnection at NASS level;
    - Interconnection ad RACS level;
    - NGN Interconnection could also occur with other PSTN/ISDN networks (non IP networks). This kind of interconnection can be considered as an inter-working scenario between NGN with legacy networks and as such already covered by other specifications.
- Interconnection at the Service layer (PES, IPTV and IMS are the current service layer subsystems).

Moreover, all kind of NGN interconnections can be recognized as one of the following types:

- Service Oriented Interconnection (SoIx), characterized by the presence of the service-related signalling (mandatory) in order to enable the end-to-end service awareness; and
- Connection oriented Interconnection (CoIx) that characterized by the absence of the service-related signalling. This implies that there is no service awareness in CoIx Interconnection.

Finally Both SoIx and CoIx can also be "direct interconnection", which refers to the interconnection between two network domains without any intermediate network domain, or "indirect interconnection", where interconnection between two network domains is achieved by means of one or more intermediate network domain(s) acting as transit networks. The intermediate network domain(s) provide(s) transit functionality to the two other network domains.

4.2 Main NNI scenarios relevant for security consideration

The following clauses describe the main use cases related to the TISPAN NGN NNI interconnection. Only the scenarios described in this clause will be taken into consideration for the scope of the present document.

4.2.1 Direct SoIx

The direct SoIx [i.6] foresees the communication of signalling (mandatory) and bearer (optional) directly between two operators without any intermediary.

Figure 1 shows the SoIX reference model and shows the relevant reference point involved (i.e. Ic or Iw and Iz) in the interconnection between two different operators. The red ovals highlight the two kind of SoIX, one related to the Ic and the other to the Iw reference point (the Iz reference point could be missing since it is optional in the SoIx):

- **SoIx Interconnection interface** includes at least Ic and Iz reference points between two interconnected domains that have same or compatible service control sub systems/domains.

- **SoIx Interconnection interface with Interworking** includes at least the Iw and Iz reference points between two interconnected domains that have non-compatible service control sub systems/domains.

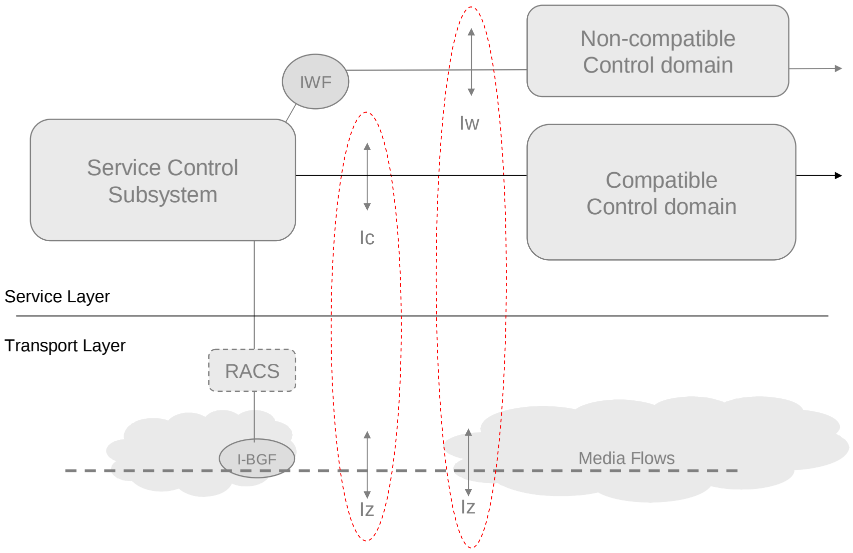
IWF
Non-compatible Control domain
Iw
Service Control Subsystem
Compatible Control domain
Ic
Service Layer
Transport Layer
RACS
I-BGF
Media Flows
Iz
Iz

Figure 1: SoIx reference model

TS 181 005 (V2.4.1) [i.7] "Service and Capability Requirements" reports the security requirements that SoIx addresses:

- Lawful interception.
- Support of appropriate privacy.
- Support of authorization.
- Support of authentication and access control.
- Support of communications and data security (including integrity and confidentiality).
- Support of DoS protection.

5 NGN Reference points and current security mechanisms

This clause contains a review of the main aspects that have been defined in the current specification for the security of the NGN NNI interconnection. Since there is not a single point of reference, the present clause tries to identify the most relevant items where described, and tries to give an overall picture of the matter.

5.1 TISPAN NNI interconnection security review

The main security mechanisms and concepts defined in the current TISPAN specs (NGN release 2) related to the security of the NNI are the following:

- Security Domain [i.1] and [i.2].
- Security Gateway Function (SEGF) [i.1] and [i.2].
- Main reference points defined at NNI level: Za, Zb, Ic, Iw and Iz [i.2].
- Topology-Hiding Inter-network Gateway (THIG) [i.1] and [i.2].

- Lawful Interception [i.3].
- Prevention of unsolicited communication [i.4], although no specific NNI interconnection analysis has been preformed.
- NAT and firewall traversal [i.13], that have been analyzed only from the UNI point of view.

The SEGF could be seen as the most relevant security element involved in the interconnection of NGN at NNI. The SEGF concept is endorsed from the TS 133 210 [i.5] but the TISPAN SEGFs may include filtering policies and firewall functionality not required by 3GPP. The SEGFs within each security domain protect the exposed interfaces between operators and ensure that a security policy among security domains is enforced (currently such a inter security domain policy is not standardized and is left to the discretion of the roaming agreements of the operators). The outbound NGN traffic from an operator cannot by pass the SEGF and NGN operators operate NDS/IP Za interface between SEGFs (which foresees the usage of IKE and IPSEC ESP tunnel).

The reference points involved in the interconnection between different Operators and protected by the SEGF are the Ic (for IMS SIP protocol), Iw (for non-IMS signalling protocol such as IETF SIP) and the Iz (the bearer, e.g. RTP). Although all the outbound/inbound traffic cannot by pass the SEGF and the Za is mandatory to implement, only the interconnection reference points related to the signalling (Ic and Iw) is protected within the IPSEC tunnels, whereas the bearer (Iz) will be not encapsulated in the IPSEC tunnels. Actually only the Ic reference point is required to be protected as defined in TS 133 210 [i.5] (e.g. SEGF and IPSEC), whereas TLS is optionally suggested for Iw [i.2] and the security of Iz is out of the scope of the TISPAN security architectures. To complete this overview it could be important to note that the THIG (Topology Hiding) function is defined to be performed by the I-CSCF (and so only for the IMS services) and that the I-BGF may provide the CC-IIF (Content of Communication Internal Intercept Function) for the lawful interconnection capabilities [i.3].

The following picture (figure 2) shows what currently have been defined for the security of the NGN NNI interconnection (up to NGN release 2). Although no specific statements have been defined for the Iw and Iz referent point, it is assumed that:

- Iw and Ic are integrity (mandatory) and confidentiality protected (optionally, unless IMS session keys are exchanged between the operators) by an IPSEC tunnel.
- The TS 187 003 [i.2] specification does not address the possible issues due to the TLS usage suggested for the protection of the Iw (e.g. firewall, i.e. SEGF, and NAT traversal issues for the bearers);
- Iz flows unprotected between the two operators (the SEGF does not take any action for the protection of the communications).
- The SEGF is mainly an IPSEC gateway with a non standardized packet filtering (or stateful inspection) firewall capability.
- Important security related functions such as NAT traversal, THIG, TLS, Lawful Interception have been defined to be implemented within other functional entities (or not yet defined as for the media security).

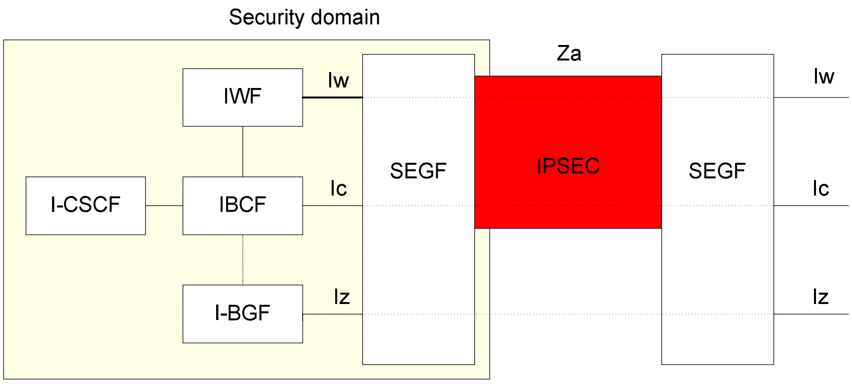

Figure 2: Tispan security for NNI interconnection

To be noted that the TS 133 210 Network Domain Security [i.5] refers to security within a NGN operator domain and between NGN operator domains that have a fixed roaming agreement. Hence it could be possible that other interconnecting scenarios needs (e.g. transit operator) are not well addressed.

5.2 TLS for the security of the NNI interconnection

The signalling at the NNI could be protected by means of TLS [i.9]. In fact, according to clause 6.5 of TS 133 203 [i.10], TLS [i.9] may be used to protect the SIP signalling (as specified in RFC 3261 [i.18]) between IMS CSCF and a proxy located in a foreign network (non-IMS network). The NDS/AF [i.11] aims at complimenting NDS/IP [i.5] by providing a PKI that is built on top of manual cross-certifications between operators. Hence in the case of TLS, NDS/AF concentrates on authentication of TLS entities across inter-operator links. TLS is specified for inter-operator communications between IMS and non-IMS networks TS 133 203 [i.10], clause 6.5 and on the Zn' interface in GBA TS 133 220 [i.17]. Authentication of TLS entities across intra-operator links is considered an internal issue for operators.

The general architecture for authentication of TLS entities is illustrated in figure 3.

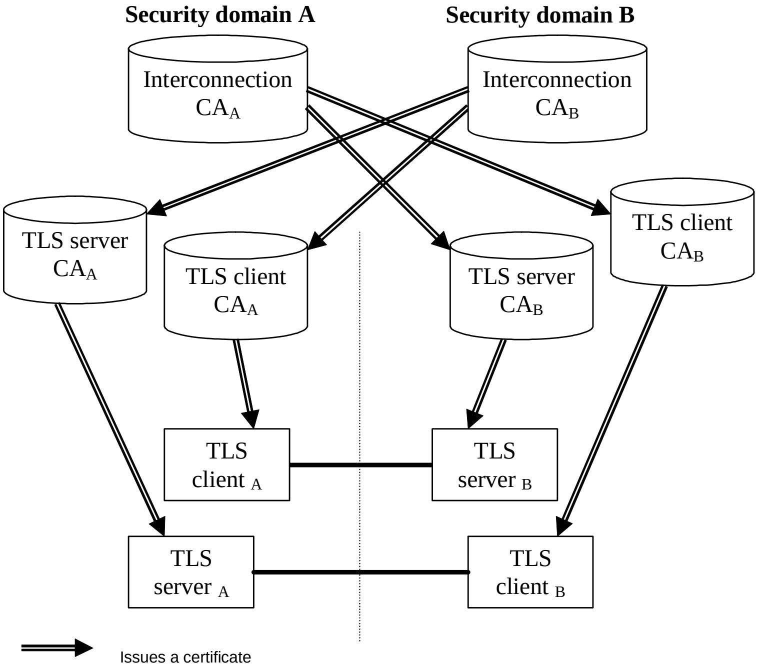

Figure 3: Trust validation path in the context of TLS

5.3 SBC for the NNI interconnection security

A session border controller (SBC) is a commercial device used by Service Providers and Operators to increase the control over the signalling and the media at the border of their VoIP network infrastructures. SBC implements many security features such as DOS prevention, encryption of the communications (IPSEC and TLS), NAT traversal and lawful interception. Hence such devices typically implement different functionalities mapped to different NGN elements. Moreover, within the TISPAN architecture, it is possible to distinguish between two different types of SBC, the Access SBC and the Interconnect SBC. The former faces directly the end-user (e.g. managing the security of the Gm), whereas the latter is used to interconnect with other networks (i.e. NNI).

The following figure 4 shows a possible mapping the typical security features of the Interconnect SBC to the corresponding TISPAN NGN elements.

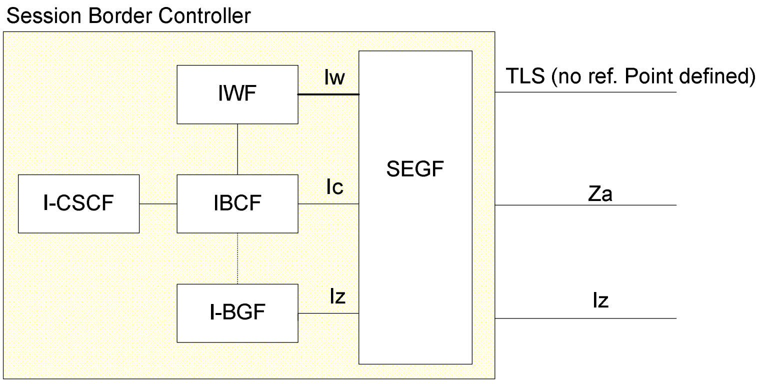

Figure 4: SBC NNI security functions mapped on the TISPAN architecture

The Interconnect-type SBC addresses the security needs at the boundary of the networks and it is a superset of the SEGF because it integrates the security features different elements of the TISPAN architecture:

- Inter-Working Function (IWF): provides interworking between NGN using different signalling profiles (e.g. RFC 3261 [i.18] SIP). IWF implements TLS for the protection of the communications. In fact many SBCs are able to manage TLS connections.
- Interconnect Border Gateway Function (I-BGF) – manages the pinholing for firewall and NAT traversal. It controls access by packet filtering on IP address/port and opening/closing gates (pinholes) into the network. It uses Network Address and Port Translations (NAPT) to hide the IP addresses/ports of the service elements in the TISPAN core.
- Interconnect Border Control Function (IBCF): interacts with I-BGF for the control of the transport layers for pinhole firewall, NAPT. SBC with distributed architecture usually are split into two separate components: one component manages the signalling (implementing the IBCF), whereas the other manages the bearers (implementing the I-BGF).
- Interrogating-CSCF: provides security for the TISPAN core by implementing a Topology-Hiding Inter-network Gateway (THIG) sub-function.
- Security Gateway Function (SEGF): implements the protection (integrity and optionally confidentiality) of the signalling between two IMS Operators. Within TISPAN the SEFG is also able to enforce specific security policy, although this function is not standardized or described. Commercial SBCs define different type of policies that could be defined and enforced, to implement e.g. rate limiting and other kind of DoS protection.

Hence, the deployment of a SBC at the NGN interconnection permits to off-load the security features from different NGN elements (or functions) and centralize them in a single element (regardless of the actual SBC architectures: single element or distributed). The following table (table 1) summarizes the main security features for the security of the NNI to be implemented within a interconnect SBC. A SBC compliant with the TISPAN specification implements the required features as described in the "NGN standard(s)" column.

Table 1: SBC security features for NNI

Security feature	Note	NGN Standard(s)
Topology Hiding (THIG)	THIG permit to hide the internal structure of the NGN networks by encrypting specific fields of the SIP signalling	TS 124 229 [i.12] clause 5.3.3.
NAT/NPT Traversal	NAT and PAT at the NNI are primarily aimed to protect the internal topology of the network.	No standard way defined for NNI. See note 1.
(D)DOS protection	Many mechanisms are possible, such as rate-limiting of the incoming traffic, block of malformed packet, etc.	No standard way defined for NNI.
SPIT detection/blocking	The NGN interconnection can be one of the most important driver used by spammers to spread their business.	No standard way defined for NNI. See note 2.
IPSEC	IPSEC (Za reference point) is used only to protect the signalling.	TS 133 210 [i.5]. The Za foresees integrity mandatory, confidentiality optional.
TLS	TLS can be used for the signalling only, but only when the interconnection is with non-IMS operator	TS 133 310 [i.11].
Media Security	The real-time flows could be eavesdropped or manipulated, especially when interconnect though public networks	No standard way defined for NNI. See note 3.
Lawful Interception	Whenever required by the regulator.	TISPAN TS 187 005 [i.3]
Security Policy enforcing (firewalling)	The SEGF is an extension of the 3GPP SEG and foresees the possibility to define security policy beyond the IPSEC functionality	No standard way defined for NNI.
DNS and ENUM Security	A secure environment is essential to all communication providers to facilitate I-ENUM. As network operations are totally dependent upon the reliability and security of routeing information. The exposure of that information, or of interconnection points potentially poses a threat to the security and stability of any network [i.8].	No standard way defined for NNI.
NOTE 1: TISPAN TR 187 008 [i.13] describes the problem from the UNI point of view. NOTE 2: TISPAN TS 187 015 [i.16] describes the issue from the UNI (CND and NGCN) point of view. NOTE 3: The current TISPAN TR 187 007 [i.14] and TS 133 328 [i.15] are focused on UNI.		

History

Document history		
V3.1.1	February 2011	Publication