ETSI TS 187 021 V3.2.1 (2014-04)

Technical Specification

Security services and mechanisms for customer premises networks connected to NGN

Reference

RTS/NTECH-00009-SEC-CPN

Keywords

gateway, IP, 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

Important notice

The present document can be downloaded from:
http://www.etsi.org

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

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://ipr.etsi.org).

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 Network Technologies (NTECH).

1 Scope

The present document specifies the functional models and information flows (stage 2) and protocols (stage 3) which implement the security services and mechanisms required to provide security in a Customer Premises Network (CPN) to support the overall security architecture for NGN release 3. CPN security services and mechanisms are used either singly or in combination to realize the CPN security requirements specified in TS 187 001 [1] (NGN Security requirements). Reference will be made to TR 185 012 [i.1] for security mechanisms that have been shown to be appropriate for CPN environment.

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.

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

[2] ETSI TS 185 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Devices architecture and Reference Points".

[3] ETSI TS 185 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Network Gateway (CNG) Architecture and Reference Points".

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

[5] Broadband Forum TR-069 Amendment 3: "CPE WAN Management Protocol", November 2010.

[6] Broadband Forum TR-157 Amendment 3: "Component Objects for CWMP", November 2010.

[7] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

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 TR 185 012: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) Feasibility study of security mechanisms for customer premises networks connected to TISPAN NGN".

[i.2] IETF RFC 5209 (June 2008): "Network Endpoint Assessment (NEA): Overview and Requirements".

[i.3] ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture".