

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study on IPTV Security Architecture

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI TR 187 013 V3.1.1 \(2011-02\)](https://standards.iteh.ai/catalog/standards/etsi/e7185131-bbd0-427b-a758-afd550125ae5/etsi-tr-187-013-v3-1-1-2011-02)

<https://standards.iteh.ai/catalog/standards/etsi/e7185131-bbd0-427b-a758-afd550125ae5/etsi-tr-187-013-v3-1-1-2011-02>



Reference

DTR/TISPAN-07033-NGN-R3

Keywords

architecture, 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

iteh Standards
(<https://standards.iteh.ai>)
Document Preview

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2011.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™**, **TIPHON™**, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

LTE™ is a Trade Mark of ETSI currently being registered

for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	6
Foreword.....	6
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	7
3 Definitions and abbreviations.....	9
3.1 Definitions.....	9
3.2 Abbreviations	10
4 Security Requirements on IPTV Content and Service Protection.....	12
5 Identification and authentication in IPTV	13
6 Generic stage 2 model for IPTV service protection	14
6.1 Overview of model.....	14
6.2 Detailed model description.....	16
6.2.1 URK generation and delivery	16
6.2.2 SEK generation and delivery	17
6.2.3 TEK generation and delivery	17
7 Candidate Key Hierarchies for Service Protection.....	18
7.1 4-Layers Key Hierarchy	18
7.1.1 Bootstrapping Layer	19
7.1.2 Key Management Layer.....	19
7.1.3 Key Stream Layer	19
7.1.4 Traffic Protection Layer.....	19
7.2 3-Layers Key Hierarchy	19
7.2.1 Bootstrapping Layer	20
7.2.2 Key Stream Layer	20
7.2.3 Traffic Protection Layer.....	20
8 Candidate Security Models for Service Protection	20
8.1 Mapping of 4-Layers Key Hierarchy to Security Model.....	20
8.2 Mapping of 3-Layers Key Hierarchy to Security Model.....	21
9 Candidate Solutions for Service Protection.....	22
9.1 Service Protection Solution One	22
9.1.1 Functional Architecture Overview.....	23
9.1.2 Reference Points	23
9.1.2.1 KMF - UE (Kx).....	23
9.1.2.2 KMF - CEF (Ky).....	23
9.1.2.3 CEF - MDF (Kz)	23
9.1.3 Solution Description	24
9.1.3.1 Procedures for service protection deployment	24
9.1.3.2 Procedures for key providing	25
9.2 OMA BCAST 1.0 as candidate solution	26
9.2.1 OMA BCAST Functional Architecture and TISPAN IPTV.....	27
9.2.2 OMA BCAST Service and Content Protection.....	31
9.2.2A OMA BCAST Smart Card Profile adaptation to MPEG-2 TS	35
9.2.3 OMA BCAST DRM-Profile as a candidate solution.....	38
9.2.3.1 Functional Architecture Overview.....	39
9.3 Service Protection using DVB Simulcrypt approach	41
9.3.1 Functional Architecture Overview.....	42
9.3.2 Solution Description	42
9.4 MBMS as candidate solution for IPTV Service Protection.....	42
9.4.1 Summary of MBMS as candidate solution	44

9.5	User Authentication and Service Authorization and any Content Protection (UA, SA and any CP) as candidate solution.....	46
9.5.1	Open IPTV Authentication, Content and Service Protection Specification.....	46
9.5.2	OIPF SAA and CSP solutions integration into TISPAN NGN.....	48
10	Gap Analysis and Selection of Possible Solutions for Service Protection.....	50
10.1	TISPAN IPTV Security Requirements.....	50
10.1.1	Common IPTV Security Requirements	50
10.1.2	IPTV Service Protection Requirements	53
10.1.3	Non-IMS-based IPTV Security Requirements.....	54
10.1.4	Availability and DoS Protection Requirements	55
10.1.5	Other Assessment Requirements	55
10.1.5.1	Ability to address legacy IPTV head end and interworking to deployed equipment	55
10.1.5.2	OMA BCAST solution.....	55
10.1.5.3	UA, SA and any CP	56
10.2	Comparisons between OMA BCAST Smartcard Profile and MBMS solutions	56
10.3	Pros and Cons considering DRM and SmartCard Profile.....	57
11	Coexistence and Interoperability Analysis.....	59
11.1	Coexistence of pre-existing non-TISPAN IPTV protection solutions.....	59
11.1.1	DVB Simulcrypt	59
11.1.2	OMA BCAST	59
11.1.3	UA SA and any CP	59
11.2	Interoperability of service protection with content protection.....	59
11.2.1	MPEG-2 Transport Stream Protection.....	59
11.2.2	OMA BCAST	59
11.3	Service Protection Model reusing UPSF/PDBF, BSF and NAFs.....	60
12	Recommendations	62
12.1	OMA BCAST.....	62
12.2	UA SA and any CP.....	62
Annex A (informative):	Service Protection using MBMS Approach.....	63
A.1	Introduction	63
A.2	Key Architecture	63
A.2.1	Four-layered key management system.....	63
A.2.2	Root Key and the Layer 1 subscriber management key	64
A.2.3	Key architecture within ETSI-TISPAN Security architecture.....	65
A.3	MBMS-Architecture.....	66
A.3.1	MBMS and GBA.....	66
A.3.1.1	Bootstrapping server function (BSF)	66
A.3.1.2	Network application function (NAF)	67
A.3.1.3	Home Subscriber Server (HSS)	67
A.3.1.4	UE.....	67
A.3.1.5	Bootstrapping architecture and reference points.....	67
A.3.1.5.1	Reference point Ub	67
A.3.1.5.2	Reference point Ua.....	68
A.3.2	BM-SC as NAF	68
A.3.3	BM-SC Network Components	68
A.3.3.1	Membership function.....	69
A.3.3.2	Session and transmission function	69
A.3.3.3	Proxy and Transport Function	70
A.3.3.4	Service Announcement Function.....	70
A.3.3.5	MBMS Security Function.....	70
A.3.3.6	Protocol stack used by MBMS User Services.....	70
A.4	Service protection of TISPAN IMS-based IPTV using MBMS.....	71
A.4.1	Using MBMS security function for IMS-based IPTV-Service Protection	71
A.4.1.1	MBMS and BM-SC scope	71
A.4.1.2	Functional entities in BM-SC and their matching to ETSI TISPAN	72
A.4.1.2.1	Key Management Function	73

A.4.1.2.2	Session and Transmission Function	73
A.4.2	Using MBMS as IPTV R3 Protection Mechanism.....	74
A.4.2.1	General Overview.....	74
A.4.2.2	Service Protection Processes for ETSI TISPAN IMS-based IPTV R3 described in detail.....	75
A.5	GBA and ETSI TISPAN NGN Architecture.....	79
History		82

iTeh Standards

(<https://standards.iteh.ai>)

Document Preview

[ETSI TR 187 013 V3.1.1 \(2011-02\)](https://standards.iteh.ai/catalog/standards/etsi/e7185131-bbd0-427b-a758-afd550125ac5/etsi-tr-187-013-v3-1-1-2011-02)

<https://standards.iteh.ai/catalog/standards/etsi/e7185131-bbd0-427b-a758-afd550125ac5/etsi-tr-187-013-v3-1-1-2011-02>

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).

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI TR 187 013 V3.1.1 \(2011-02\)](https://standards.iteh.ai/catalog/standards/etsi/e7185131-bbd0-427b-a758-afd550125ae5/etsi-tr-187-013-v3-1-1-2011-02)

<https://standards.iteh.ai/catalog/standards/etsi/e7185131-bbd0-427b-a758-afd550125ae5/etsi-tr-187-013-v3-1-1-2011-02>

1 Scope

The present document presents the result of a study of options for the IPTV security architecture supporting TISPAN NGN Release 3 that satisfies the security requirements for IPTV given in TS 187 001 [i.1].

The present document offers the results of analysis of the options for security architecture and mechanisms to provide IPTV service protection where service protection refers to the protection offered during the period when IPTV media is transmitted in the NGN. A security architecture for a general content protection framework to allow comparison of existing content protection solutions (e.g. DRM systems) is required for the NGN, but is not covered by the present document. Content protection includes the provision of post-delivery protection of IPTV media and may include controls to ensure that the user can only use the content in accordance with the license it has been granted, e.g. the times of the content can be viewed.

NOTE: The functional architecture for IMS based IPTV without security entities conforms to TS 182 027 [i.5].
The functional architecture for dedicated IPTV subsystem without security entities conforms to TS 182 028 [i.6].

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] Void.
- [i.3] ETSI TS 181 016: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service Layer Requirements to integrate NGN Services and IPTV".
- [i.4] ETSI TS 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".
- [i.5] ETSI TS 182 027: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; IPTV functions supported by the IMS subsystem".
- [i.6] ETSI TS 182 028: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN integrated IPTV subsystem Architecture".