3GPP TR 33.803 V7.0.0 (2007-06)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Coexistence between TISPAN and 3GPP authentication schemes (Release 7)

Keywords
IMS, Security

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document studies from a security point of view the coexistence between TISPAN authentication methods (as specified in TISPAN release 1) and existing 3GPP authentication schemes, i.e. both the IMS AKA (as specified in TS 33.203 [5] and TS 24.229 [4]) and the early IMS security (as specified in TR 33.978 [6]). This document also aims to provide solutions to handle potential compatibility issues. These issues are listed in detail in section 5 of this document.

This document is meant to ensure that the same IMS core network entities can be used to support both 3GPP and TISPAN authentication schemes. In this context, rules are developed how an x-CSCF can decide from a registration request which authentication scheme to apply. If these rules are not adhered to compatibility problems may arise.

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, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2".

[3] ETSI ES 283 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3".

[4] 3GPP TS 24.229: "3rd Generation Partnership Project; Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[5] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services".

[6] 3GPP TR 33.978: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Aspects Of Early IMS".

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

[8] IETF RFC 2617 (1999) "HTTP Authentication: Basic and Digest Access Authentication".

[9] ETSI TS 183 033: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia; Diameter based protocol for the interfaces between the Call Session Control Function and the User Profile Server Function/Subscription Locator Function; Signalling flows and protocol details".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

P-CSCF: for definition see TS 23.228 [2].

S-CSCF: for definition see TS 23.228 [2].

TISPAN-aware P-CSCF: for definition see section 6.1.

Legacy P-CSCF: for definition see section 6.1.

3.2 Symbols

None are used in the present document.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

EIS	Early IMS Security
NASS	Network Access Subsystem (a concept defined by ETSI TISPAN)
NAT	Network Address Translation
NBA	NASS bundled authentication
UPSF	User Profile Server Function (a concept defined by ETSI TISPAN)

4 Requirements

- It shall be possible to deploy one IMS in a fixed (TISPAN) mobile (3GPP) convergence situation.
- As a minimum it shall be possible to serve both fixed and mobile subscribers at the same S-CSCF.
- Incompatibilities between 3GPP and TISPAN authentication schemes shall be avoided.
- The following authentication schemes are taken into account in this Technical Report:
  - IMS AKA with and without NAT traversal (as specified in TS 33.203 [5] and TS 24.229 [4]),
  - Early IMS security mechanisms (as specified in TR 33.978 [6]),
  - NASS-IMS-bundled authentication (as specified in ETSI TS 187 003 [7] and ETSI ES 283 003 [3]),
  - HTTP Digest (as specified in RFC 2617 [8] and ETSI TS 183 033 [9]) HTTP digest is applicable only for non-3GPP defined TISPAN access networks, but is not applicable and not intended for 3GPP access networks.
- Access independence is a key concept of the IMS. In order to achieve convergence this concept must be preserved. Therefore both 3GPP and TISPAN IMS specifications should consider IMS-AKA as the authentication of choice and other mechanisms only as preliminary.

5 Identified Issues

- P-CSCF procedure selection:
  - TISPAN procedures may apply only to a subset of subscribers.
  - 3GPP procedures may apply to other subset of subscribers.
  - How does the P-CSCF know which procedure to apply?
- Determination of requested authentication scheme in S-CSCF:
  - In an environment where multiple authentication schemes are used, a S-CSCF may not be able to correctly detect the requested authentication scheme to indicate to HSS/UPSF, unless certain rules are adhered to.
  - For TISPAN authentication methods, the authentication scheme indicated by S-CSCF may be overridden by UPSF.
  - So, the S-CSCF has to behave differently, depending on the authentication method. How can the S-CSCF know from the IMS registration request and, possibly, additional information, which specification to follow?
- TISPAN-aware and legacy P-CSCFs coexistence:
  - The two types of P-CSCF differ in their handling of P-Access-Network-Info headers in a security-relevant way, as described in section 6.1. This raises the following issue:
  - How can the S-CSCF, which concurrently serves both TISPAN-aware and legacy P-CSCFs, know whether a P-CSCF is legacy or TISPAN-aware?

NOTE 1: The handling of private user identities in Cx commands relating to registration requests without Authorization header remains left open in TISPAN Release 1 specifications. Therefore, proprietary solutions may be required in networks where TISPAN Release 1 IMS clients may send registration requests without Authorization header. Some of these proprietary solutions may require the I-CSCF to handle Cx commands in a way specific to TISPAN Release 1 IMS clients. In such a case the I-CSCF may use the P-Access-Network Info header to determine whether the request was sent over a TISPAN NASS network or a 3GPP network. In contrast to the procedures for the S-CSCF in section 6.2, the correctness of the information in the P-Access-Network Info header is not security-critical in the context of the I-CSCF discussed in this note.

NOTE 2: The issue mentioned in note 1 does not occur for UEs according to TISPAN Release 2 specifications as registration requests are always sent with Authorization headers.

6 Analysis

6.1 P-CSCF procedure selection

When the P-CSCF receives a registration request it shall proceed as follows:

The P-CSCF shall check whether the Security-Client header exists in the received REGISTER message:

- If the Security-Client header exists and contains "ipsec-3GPP", the P-CSCF shall behave according to TS 33.203 [5] and TS 24.229 [4].
- If the Security-Client header does not exist, and the REGISTER is received from a TISPAN access network, the P-CSCF shall behave according to ETSI ES 283 003 [3].
- If the Security-Client header does not exist, and the REGISTER is received from a 3GPP access network, the P-CSCF shall behave according to TR 33.978 [6].

The behaviour of either a TISPAN-aware P-CSCF and a legacy P-CSCF is defined as follows:

- A legacy P-CSCF will neither insert a P-Access-Network-Info header nor perform checking of "network-provided" parameter in P-Access-Network-Info header sent by the UE.

- If the request is received via a TISPAN access network a TISPAN-aware P-CSCF shall insert a P-Access-Network-Info header containing the "network-provided" parameter and remove any such header containing the "network-provided" parameter sent by the UE, as specified in ETSI ES 283 003 [3].

- If the request is received via a 3GPP access a TISPAN-aware P-CSCF shall remove a P-Access-Network-Info header if it contains the "network-provided" parameter, as specified in ETSI ES 283 003 [3].

- If the request is received via a 3GPP access a TISPAN-aware P-CSCF shall not insert a P-Access-Network-Info header.

NOTE: According to TS 24.229 [4] the UE includes a P-Access-Network-Info header in registration requests, which is handled transparently by the P-CSCF, and, hence, an S-CSCF could receive a P-Access-Network-Info header with false information inserted by the UE. This could negatively impact the security of TISPAN authentication schemes. Therefore removal of a P-Access-Network-Info header containing the "network-provided" parameter is required.

How the P-CSCF knows the access network type of a specific network interface is implementation-dependent (e.g. it can know the access network type from different UE IP address ranges or by using different network interfaces for different access network types).

6.2 Determination of requested authentication scheme in S-CSCF

6.2.1 Stepwise approach

It is proposed that the S-CSCF distinguishes among authentication methods using the following three steps. How these steps are performed is described in the following section.

- **Step 1:** the S-CSCF first checks whether the IMS registration request relates to IMS-AKA or not. In the case of IMS-AKA, the S-CSCF shall behave according to TS 33.203 [5]. Otherwise, the S-CSCF proceeds to step 2.

- **Step 2:** for a non-IMS-AKA registration request, the S-CSCF next checks whether the request relates to a 3GPP authentication method (i.e. Early IMS) or a TISPAN-defined authentication method. In the case of Early IMS, the S-CSCF shall behave according to TS 33.978 [6]. In the case of TISPAN-defined authentication methods, the S-CSCF proceeds to step 3.

NOTE: A distinction between 3GPP and TISPAN authentication methods is required at this stage, because a TISPAN-specific Cx-MAR-request (e.g. using the value "unknown") will be handled by the UPSF (defined by TISPAN) and not the HSS (defined by 3GPP), and the UPSF will not be able to handle 3GPP authentication methods (i.e. Early IMS) and vice versa.

- **Step 3:** In step 3, the S-CSCF follows the TISPAN specification ETSI TS 183 033 [9] for handling non-IMS-AKA registration requests.

6.2.2 Mechanisms for performing steps 1 to 3

Step 1:

The S-CSCF checks for the presence of an Authorization header, and, if present, checks further for the presence of an "integrity-protected" flag within this header. If the flag is present the S-CSCF concludes that the IMS registration request relates to IMS-AKA.

Step 2:

This approach makes two assumptions:

1) The S-CSCF knows (cf. Configuration based solution described in section 6.3), which P-CSCFs are TISPAN-aware.

2) It is ensured that legacy P-CSCFs connect only to 3GPP access networks.

Based on the above assumptions and the P-Access-Network-Info handling procedure described in section 6.1, The S-CSCF then proceeds as follows:

If there is no Authorization header, and there is either:

- no P-Access-Network-Info header containing the "network-provided" parameter or

- the registration request is received from a legacy P-CSCF,

then Early IMS is used.

Otherwise, if either

- there is an Authorization header with no "integrity-protected" flag or

- there is no Authorization header, and the access-type parameter in the P-Access-Network-Info header containing the "network-provided" parameter represents TISPAN access, and the request is received from a TISPAN-aware P-CSCF,

then the S-CSCF proceeds to step 3.

Step 3:

This step is handled according to ETSI TS 183 033 [9].The remaining authentication methods that the S-CSCF may still have to discriminate in this step are all TISPAN-specific methods, i.e., not used in 3GPP networks.

6.3 Coexistence of TISPAN-aware and legacy P-CSCFs

This section introduces a configuration-based solution, which enables an S-CSCF, to serve both TISPAN-aware and legacy P-CSCFs.

Configuration-based solution:

The S-CSCF shall be configured in such a way that it knows which P-CSCFs are TISPAN-aware, according to section 6.1. The S-CSCF knows the P-CSCF which forwarded the registration request from the Via header.

NOTE 1: Both EIS and NBA require the P-CSCF to be in the home network. This may help in realising the configuration-based solution.

NOTE 2: A protocol-based solution may be added in a future release of this specification. In such a solution, a TISPAN-aware P-CSCF could include an indication about its capability to handle the "P-Access-Network-Info" header correctly, according to section 6.1, in an appropriate header field.

Annex A:
Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
2007-05	SP-36	SP-070342	-	-	-	MCC editorial update for presentation to TSG SA#36 for approval	1.1.0	2.0.0
2007-06	-	-	-	-	-	Approved at SP-36 and updated to version 7.0.0	2.0.0	7.0.0