3GPP TSG SA WG3 Security — S3#26 **S3-020603**
19- 22 November 2002, Oxford, UK

3GPP TR ~~ab~~33.cde ~~Vx~~V0.2~~y~~.0~~z~~ (~~yyyy~~2002-

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Service and System Aspects~~<TSG name>~~;
Presence Service~~<Title 1~~;
Security;~~Title 2>~~
(Release 6)

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

The present document has been developed within the 3rd Generation Partnership Project (3GPP ™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP ™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Remove GSM logo from the cover page for pure 3rd Generation documents.

Select keywords from list provided in specs database.

Keywords

<keyword[, keyword]>

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

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.

© 2002, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC).
All rights reserved.

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.

Introduction

This TR defines the security architecture, trust model and requirements for the presence services. Presence services enable the spreading of presence information of a user to users or services. A presence entity or presentity comprises the user, users devices, services and services components. It is the intention that this platform will enable new services like e.g. enhancement to chat, multimedia messaging, cinema ticket information, the score of a football game and so on.

A user has the possibility to control if her or his information shall be available to other users or services. This control is possible to achieve with high granularity e.g. explicitly define which user or users and services that shall have access to presence information.

A presentity is an uniquely identifiable entity with the capability to provide with presence information and it has only one principal associated with it. Hence a principal is distinct from all other principals and can be e.g. a human, organisation, program or even a collection thereof. One example of such a relation is when the presentity is a terminal and the principal of the terminal is the subscriber. A watcher is also an uniquely identifiable entity but with the aim to fetch or request information about a presentity. There are access rules that set the rules for the presence service how presence information gets available to watchers.

Presence information consists of a number of elements or presence tuples as defined in [XXXX].

1 Scope

~~*This clause shall start on a new page. No text block identified. Should start:*~~

The present document describes the Stage 2 description (security architectural solution and functionalities) for the Presence Service, which includes the elements necessary to realise the stage 1 requirements in 3GPP TS 22.141 [2] and 3GPP TS 23.141 [3].

The present document includes information applicable to network operators, service providers and manufacturers.~~The present document …~~

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 22.141: "Presence service; Stage 1".

[3] 3GPP TS 23.141: "Presence service; Stage 2".

[4] Common Presence and Instant Messaging (CPIM) Presence Information Data Format, Internet Draft http://www.ietf.org/internet-drafts/draft-ietf-impp-cpim-pidf-05.txt, May 2002

Editor's note: The above document is not yet published as an RFC, where possible the reference should be converted to an RFC prior to approval should this document be converted to a Technical Specification.

[5] Session Initiation Protocol (SIP) Extensions for Presence, Internet-Draft http://www.ietf.org/internet-drafts/draft-ietf-simple-presence-07.txt, May 2002

Editor's note: The above document is not yet published as an RFC, where possible the reference should be converted to an RFC prior to approval should this document be converted to a Technical Specification.

[6] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[7] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[8] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[9] IETF RFC 3265: "Session Initiation Protocol (SIP) Event Notification"

[10] A SIP Event Package for List Presence, Internet-Draft, http://search.ietf.org/internet-drafts/draft-ietf-simple-presencelist-package-00.txt, June 2002

Editor's note: The above document is not yet published as an RFC, where possible the reference should be converted to an RFC prior to approval should this document be converted to a Technical Specification.

[11] IETF RFC 2778: "A Model for Presence and Instant Messaging".

[12] IETF RFC 2779: "Instant Messaging / Presence Protocol Requirements".

~~[<seq>] <doctype> <#>[([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".~~

~~[1] 3GPP TR 41.001: "GSM Release specifications".~~

~~[2] 3GPP TR 21 912 (V3.1.0): "Example 2, using fixed text".~~

3 Definitions, symbols and abbreviations

Delete from the above heading those words which are not applicable.

Subclause numbering depends on applicability and should be renumbered accordingly.

3.1 Definitions

For the purposes of the present document, the [following] terms and definitions [given in ... and the following] apply.

Definition format

***<defined term>**: <definition>.*

example: text used to clarify abstract rules by applying them literally.

3.2 Symbols

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

Symbol format

<symbol> <Explanation>

3.3 Abbreviations

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

Abbreviation format

<ACRONYM> <Explanation>

4 Security Requirements for Presence Service

In this section some important requirements that will or may affect the security solutions for presence are identified.

4.1 Roles in Presence Architecture

In this section the different roles that come into play for presence are identified and described.

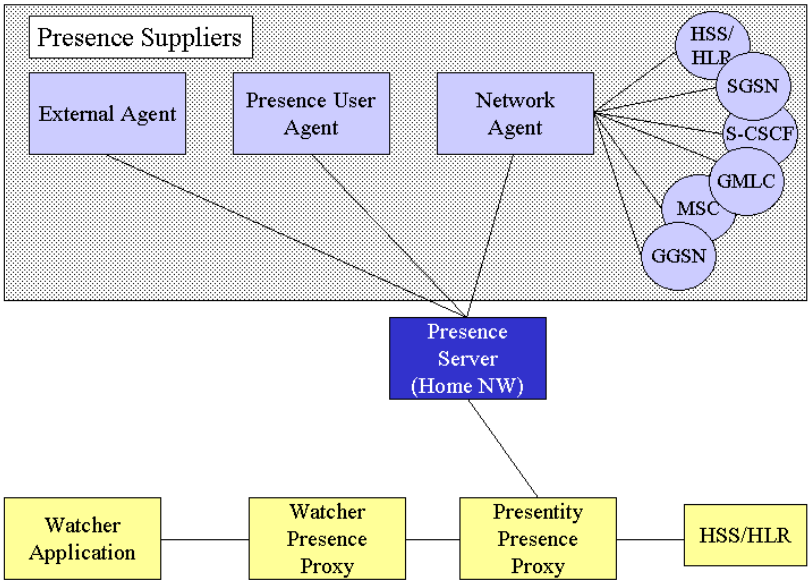


Figure 1 Overview of the presence architecture

The architecture as defined in [3] to support presence service contains a number of roles. This architecture is very general in nature and it can be applied on e.g. IMS.

The following roles have been identified which substantiates the development of the security architecture for Presence:

1. Information sources - Suppliers
    a. External Presence Supplier (External Agent)
    b. User Agent Presence Supplier (Presence UA)
    c. Network Presence Suppliers
        i. HSS
        ii. S-CSCF
        iii. MSC/VLR
        iv. SGSN
        v. GGSN
        vi. GMLC
2. Information sinks
    a. Watcher applications in terminals (fetcher or subscriber)
    b. Watcher applications in Application Servers (fetcher or subscriber)
    c. Presence Server
    d. Legal Interception application
3. Information proxy provider
    a. Watcher presence proxy
    b. Presentity Presence proxy
4. Customer
    a. Principal
    b. Watcher
5. Attacker

4.1.1 Watcher application

- An application that can request and obtain presence information
- In IMS a watcher application can be located in the UE registered and the UE is registered in the S-CSCF
- In IMS a watcher application cab be located in an AS behind an ISC interface

4.1.2 Watcher presence proxy

- Authenticates the Watcher
- Generates accounting information

4.1.3 Presentity Presence Proxy

- Generates accounting information
- Determines the identity of the presence server

4.1.4 Presence Server

- Transforms presence related information from different sources to on single presence document
- Allows user to subscribe and fetch presence information
- Provides with presence information to any watcher application
- Provides with presence information to allowed watcher applications specified in a list

4.1.5 Presence User Agent

- Sends presence information to the presence server
- Manages Access Rules
- Can be located in the UE
- Can be located in the network e.g. for SMS or WAP scenario

4.1.6 Network Agent

- May receive presence information from HSS, S-CSCF, MSC, SGSN, GGSN and GMLC
- Sends presence information to the Presence Server in the Home Network

4.1.7 External Agent

- Supplies presence information from external networks
- Sends presence information to the Presence Server in the Home Network

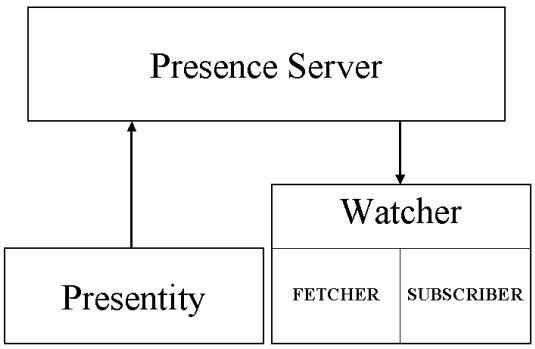
4.2 Scenarios and assets

The scenarios below are basically taken from [RFC2778]:

- The Presence Server accepts, stores and distributes presence information

- The Watcher receives presence information from the presence server
- The Presentity provides with presence information

Here it has not been given from what sources apart from the Presentity that provide with information to the Presence Server. According to [RFC2778] the Presence Server (or Presence Service) has Watcher information as well. This information is based on what activities the Watcher is undertaking e.g. acting as a fetcher (i.e. poller) or subscriber. The presence server may also distribute watcher information to watchers. Whenever the presence information is changed it is distributed to subscribers, cf. figure below.



In order to identify the threats and security requirements we need to identify the assets in presence.

The information that is the key asset in the presence service is of course the presence information. This information is used by watchers e.g. watcher applications. It seems that in order for the presence server to 'sell' presence information it should be available, reliable and accurate. If the presence server cannot guarantee this it could mean that the reputation of the presence server owner could be damaged. Furthermore since external 3rd parties can also provide with information to the presence server a general business model means that also these players would regard their information as an asset in particular if the information is based on raw data which is gathered and processed. Hence the identified assets are:

- The Presence and Watcher Information – especially the aspects related to user privacy. This asset is assumed to be very valuable for the user.
- The reputation of the owner of the Presence Server
- The Presence Information gathered and supplied by Suppliers

What is interesting is how these assets are exchanged i.e. between what Roles and over what interfaces.

4.~~2~~3 Trust model

The Presence Server is the central node in the Presence architecture. It will receive and manage information from different sources. The Presence Server shall authorise who can get access to what information. Clearly everyone in the system shall trust the Presence Server.

The network nodes that provide information via the Presence Network Agent either reside in the Visited Network or in the Home Network. It is reasonable to adopt the existing trust model we have in e.g. R'99 where the SGSN is trusted to authenticate a 3G subscriber via the roaming agreement. It seems therefore fair to assume that the information provided by those network elements can be trusted i.e. that both the HN and the VN can ensure that non-authorised entities cannot tamper with the data in the node. Hence the Presence Server trusts the Network Presence Suppliers, the Presentity Presence Proxy and the Watcher Presence Proxy.

The Presence User Agent supplies the presentity information to the Presence Server and it will also manage the access rules. From the presentity point of view there will be a number of watcher applications that request or subscribe to presence information. Some of these watchers may be known to the Presentity e.g. friends or colleagues whereas others are not known beforehand or are even anonym. Since the presence information will potentially reveal sensitive

information about the Presentity e.g. user status and location, not all the watchers are trusted by the presentity. Some watchers are only trusted to the extent that they can get information about user status but not location. Hence the trust of the presentity to a watcher might be total, non-existing or anything in between.

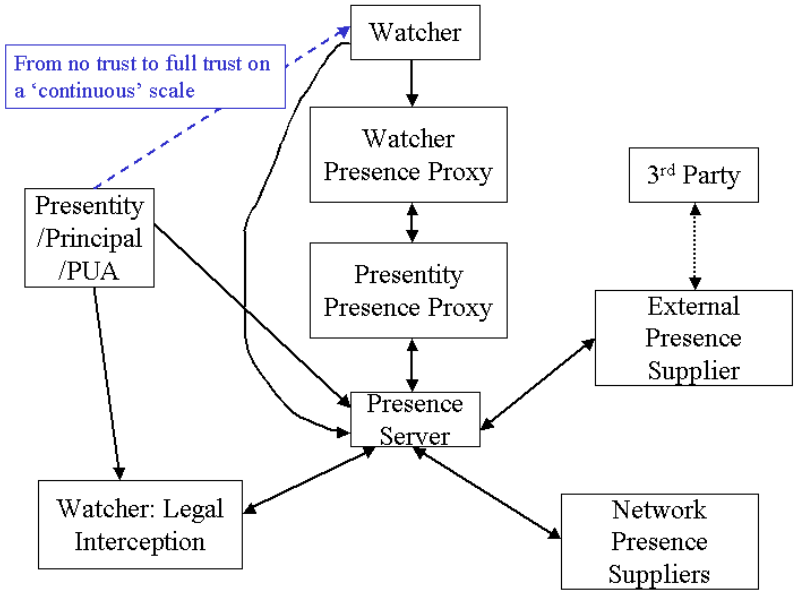
It is envisioned that the presence information will be in the interests of the legal authorities and that operators need to ensure that there are mechanisms in place making it possible to collect this information e.g. in a Legal Interception Watcher. If such an application is applied the Presentity can do nothing more than to have trust on that application.

A Watcher Presence Proxy will proxy information between the Watcher and the Presence Server in both directions. The proxy will generate billing and charging information and has a relationship with the Watcher e.g. in terms of a subscription. A Watcher shall trust a Watcher Presence Proxy although the proxy might very well be distributed in the Visited Network and the Home Network.

The Watcher Presence Proxy shall proxy the information towards the Presence Server via a Presentity Presence Proxy. Clearly these two nodes need to trust each other.

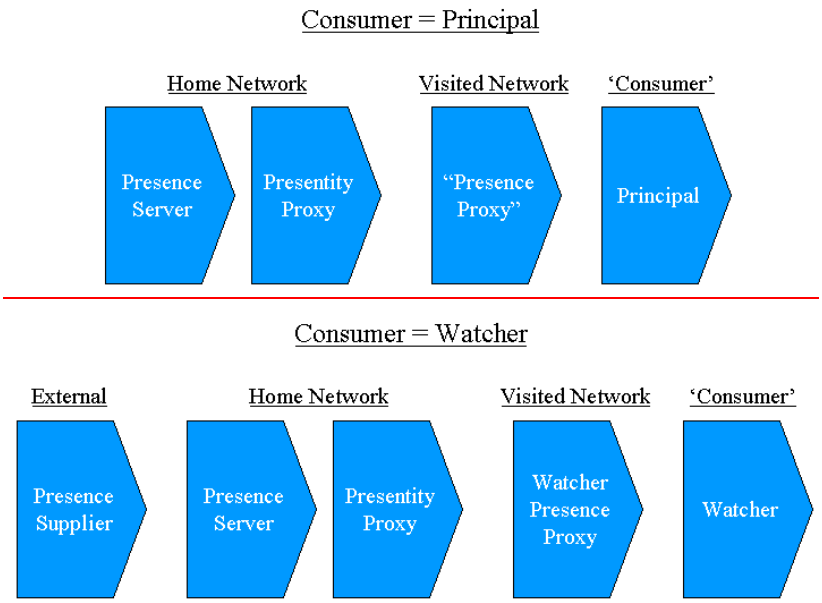
The following trust relationships between the roles that are participating in Presence are then proposed based on the above (as captured in the figure below):

- The Presence Server trusts the Network Presence Suppliers
- The Presence Server trusts the Presentity Presence Proxy
- The Presence Server trusts the Watcher Presence Proxy
- All Roles (modulo the Attacker) trust the Presence Server
- The Principal may have no trust, low trust, medium trust (scale not to be defined!) or trust in Watchers
- The Principal trusts the Legal Interception application
- The Watcher trusts the Watcher Presence Proxy
- The Watcher trusts the Presence Server
- The Watcher Presence Proxy trusts the Presentity Presence Proxy



It is assumed that a 3rd party is not necessarily situated in a 3G network and therefore no trust establishment has been stated here. Presumably any operator setting up a relationship with a 3rd party needs to ensure that necessary considerations around trust and security measures are considered.

~~According to section 4.1 the value add points were charging information is generated are the Presentity Presence Proxy and the Watcher Presence Proxy.~~



~~**Figure 2 Overview of the value system**~~

~~A principal may register to provide information for watchers to use the Presence Service and also create the required access rules. The principal may register himself as a presentity or/and a watcher. The registration may be general i.e. without prior arrangements or pre-arranged e.g. the service provider has issued login name/password. The registration process can be viewed as a value added service that an operator might want to charge for.~~

~~A watcher can take different roles e.g. fetcher, poller or subscribed watcher that requests notifications of changes in presence information. Whenever presence information is passed to the watcher this is a value added service and shall be charged for. As already mentioned charging information will be available in the Presentity Presence Proxy and the Watcher Presence Proxy.~~

~~There are different Presence suppliers i.e. external agents, Presence User Agent and Network agent. An external agent provides with information to the home network, which adds value to the services and hence might require some charging. A user agent updating the presence information wants to do that such that watchers get latest information and for this the home network might want to charge the user agent.~~

~~- A watcher requires some trust in the Watcher Presence Proxy, Presence Server, Presentity Proxy and the Presence Supplier~~

~~- There is a trust relationship between the Home Network and the Visited Network~~

~~- The Home Network needs to trust the presence supplier~~

~~- A principal has trust in the Visited Network as well as the Home Network~~

~~*[Editors Note: This list is not exclusive and needs further review and updates]*~~

4.3 Threats

[Editors Note: In this section different potential threats that need to be mitigated should be stated.]

An attacker eavesdrops, modifies, masquerades, replays or performs Denial of Service Attacks over the different P-Interfaces.

- It is estimated that with low probability that the attacker can succeed with any of these attacks over the Ph, Pi, Pc, Pg, Pg, Pl, Pk, and Px Interfaces .
- It is estimated that the attacker with higher probability can succeed with any of these attacks over the Peu, Pen, Pex and the Pw Interface if no security measures are used.

These attacks modulo Denial of Service attacks would have the following impacts if they succeed:

- Eavesdropping would have an impact on the Privacy asset
- If an attacker modifies the Presence information then it would impact on the Reputation of the Presence Server owner since the information would no longer be accurate nor reliable.
- If an attacker replays Presence information it would also impact on the Reputation of the Presence Server owner since the information would no longer be accurate nor reliable.
- If the Attacker succeeds to masquerade as being a valid Presentity the Privacy of that Presentity is impacted as well as the Reputation of the Presence Server owner
- If the Attacker succeeds to masquerade as being a valid and trusted Watcher the Privacy asset is impacted

It is estimated that with high probability the Attacker can interfere with the interface between the 3rd party and the Presence External Agent if no security measures are installed

- Eavesdropping would have an impact on the Privacy asset

If an attacker modifies the Presence information then it would impact the Reputation of the Presence Server owner since the information would no longer be accurate nor reliable

4.4 Requirements

4.4.1 General

The use and access to the presence service shall be supported in a secure manner. It shall only be possible for the presence information to be supplied and/or updated by the presentity or the home environment ~~as identified in clause 5 "High Level Requirements"~~.

The presence service shall support measures to detect and prevent attempts to maliciously use or abuse the services. It shall be possible to authenticate presentities and/or watchers at any time.

It shall be possible to authenticate a principal before allowing registration to the presence service.

It shall be possible to authenticate a watcher requesting access to the presence service. Existing security mechanisms as well as mechanisms specific to presence service may be used.

It shall be possible to authorise a watcher's watcher-subscription request to a presentity's presence information.

It shall be possible to protect the following items from attacks (e.g., eavesdropping, tampering, and replay attacks):

- Presence information and notifications
- Requests for presence information, e.g., requests for subscription and requests for presence information retrieval.

[Editors Note: These ~~are~~ requirements above are copied from [3~~1~~] and require a review and updates]

There is a need to protect the Peu and the Pw interfaces with security measures offering confidentiality, integrity as well as replay protection. The need for similar security in Pen and Pex interfaces in for further study. Furthermore since using a 'continuous' scale the Presentity shall be able to set access rules in a general way such that it can decide what information shall be available to what Watcher. However the Presentity needs to allow that a legal interception Watcher is authorised to collect information about the Presentity such that the Presentity is not even aware of it. This shall include that the Presentity shall be able to control the authenticity of a watcher i.e. that the information is controlled via e.g. a password based mechanism. The Presentity if it desires shall also be notified and even to authorise end-to-end Watchers. The Presentity shall also have the possibility to check what watchers have received what presence information from a Presence Server.

These high-level requirements are collected in the following list:

1) The Peu interface shall be integrity protected, confidentiality protected and offer replay protection.

2) The Pw interface shall be integrity protected, confidentiality protected and offer replay protection. Anonymity services shall be provided.

3) The Presentity shall be able to set the access rules in a general manner in the Presence Server for all Watchers except the legal interception application

4) The Presentity should be able to require that a Watcher shall be authenticated in the Presence Server

5) The Presentity should be able to authorise a Watcher request end-to-end

6) The Presentity should be able to have access to a log

In addition to the previous requirements, the Pen and Pex interfaces may require integrity and replay protection.

4.4.2 IMS related

The following working assumptions related to Presence have been defined:

1) Peu: Existing IMS security architecture fulfils the security requirements related to authentication, integrity protection, replay protection and anonymity.

2) Ph: No additional security requirements.

3) Pi: No additional security requirements.

4) Pc: No additional security requirements.

5) Pg: No additional security requirements.

6) Pk: No additional security requirements.

7) Pl: No additional security requirements.

8) Pw: Existing IMS security architecture fulfils the security requirements related to authentication, integrity protection and replay protection.

The following interfaces are left FFS:

1) Pex: Security between PEA and external information source should be further studied.

2) Pex, Peu & Pen: Threats and potential solutions for false presence information inside the network should be further studied.

3) Peu & Pw: IMS may need to be enhanced by IPsec encryption between UE and P-CSCF in order to fulfil the confidentiality requirement.

4) Peu & Pw: The degree of anonymity provided by ‘anonymous IMPU’ should be further studied.

5) Peu & Pw: Ability of non-IMS accesses (e.g. WAP/SMS/WV) to fulfil the security requirements should be further studied.

6) Pw: The Presence Server may need additional mechanism for authenticating the Watchers. For example, the Presentity may provide passwords for Watcher authentication.

7) Pw: The Presentity may need additional mechanism for authenticating the Watchers. For example, the Watcher may provide a token or electronic signature for authentication.

8) Pw: IMS may need to be enhanced by a security mechanism for the Watcher to request anonymity.

It is suggested that LSs related to the following issues are sent to other 3GPP working groups:

Peu: It is not clear yet which protocols will be used in Peu interface. Peu may include protocols for web access (e.g. HTTP for access list manipulation and registrations), and consequently there may be a need for additional security.

5 Security architecture

6 Security features

7 Secure access

8 Security mechanisms

~~"TSG <Name>" on the front page~~

~~*The following text are used for the Technical Specification Group "<**Name**>" on the front Page:*~~

~~**TSG**~~	~~**Full Name**~~
~~TSG CN~~	~~Core Network~~
~~TSG RAN~~	~~Radio Access Network~~
~~TSG SA~~	~~Services and System Aspects~~
~~TSG T~~	~~Terminals~~
~~TSG GERAN~~	~~GSM/EDGE Radio Access Network~~

~~Page setup parameters~~

~~*This clause defines the margin parameters and the header to be used.*~~

~~*Title page (= title section)*~~

~~*A4 portrait, Top: 4 cm, Bottom: 19 cm, Left: 1,5 cm, Right: 1,5 cm, Gutter: 0 cm, Header: 0 cm, Footer: 0 cm.*~~

~~*Portrait sections*~~

~~*A4 portrait, Top: 3 cm, Bottom: 2 cm, Left: 2 cm, Right: 2 cm, Gutter: 0 cm, Header: 1,5 cm, Footer: 0,6 cm.*~~

~~*Landscape sections*~~

~~*A4 landscape, Top: 2,0 cm, Bottom: 1,5 cm, Left: 2 cm, Right: 2,7 cm, Gutter: 0 cm, Header: 1,2 cm, Footer: 0,6 cm.*~~

~~*Headers and footers*~~

~~*Header*~~

~~*The following contains the master location for all headers (except for the title section). These paragraphs contain framed fields which will result in one header line and are bookmarked "header".*~~

~~*The left entry contains a possible additional document reference, e.g. "Release 1999", identified on the title page by the use of the ZGSM character style.*~~

~~**Release 6**~~

~~*The center entry is the page number.*~~

~~**10**~~

~~*The right entry repeats the title page information, identified by the use of the ZA paragraph style.*~~

~~**3GPP TR ab.cde Vx.y.z (yyyy-mm)**~~

~~*NOTE: For documents which are split into more than one file, the possible additional document reference and the title page information need to be hardcoded in all files except the one containing the title section.*~~

~~*Footer*~~

~~*The footer contains always "3GPP" (except for the title page).*~~

~~***3GPP***~~

Proforma copyright release text block

(e.g. for PICS and PIXIT Proformas)

This text box shall immediately follow after the heading of an element (i.e. clause or annex) containing a proforma or template which is intended to be copied by the user. Such an element shall always start on a new page.

Notwithstanding the provisions of the copyright clause related to the text of the present document, [tbd] grants that users of the present document may freely reproduce the <proformatype> proforma in this {clause|annex} so that it can be used for its intended purposes and may further publish the completed <proformatype>.

Abstract Test Suite (ATS) text block

This text should be used for ATSs using TTCN. The subdivision is recommended.

This ATS has been produced using the Tree and Tabular Combined Notation (TTCN) according to ISO/IEC 9646-3 [<x>].

The ATS was developed on a separate TTCN software tool and therefore the TTCN tables are not completely referenced in the table of contents. The ATS itself contains a test suite overview part which provides additional information and references.

<x1> The TTCN Graphical form (TTCN.GR)

The TTCN.GR representation of this ATS is contained in an Adobe Portable Document Format™ file (<pdf_file_name>.PDF contained in archive <zip_file_name>.ZIP) which accompanies the present document.

<x2> The TTCN Machine Processable form (TTCN.MP)

The TTCN.MP representation corresponding to this ATS is contained in an ASCII file (<mp_file_name>.MP contained in archive <zip_file_name>.ZIP) which accompanies the present document.

Annexes are only to be used where appropriate:

Annex <A>:
<Annex title>

Annexes are labeled A, B, C, etc. and are "informative"(3G TRs are informative documents by nature).

~~A.1 Heading levels in an annex~~

~~Heading levels within an annex are used as in the main document, but for Heading level selection, the "A.", "B.", etc. are ignored. e.g. **A.1.2** is formatted using ***Heading 2*** style.~~

Bibliography

The Bibliography is optional. If it exists, it shall follow the last annex in the document.

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

Bibliography format

- <Publication>: "<Title>".

OR

<Publication>: "<Title>".

Annex <X>:
Change history

It is usual to include an annex (usually the final annex of the document) for reports under TSG change control which details the change history of the report using a table as follows:

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2002~~1~~-07	SA3#24	SA3-020340			First Draft TR: Presence security Architecture~~Copyright date changed to 2001; space character added before TTC in coyright notification; space character before first reference deleted.~~	~~1.3.2~~	0~~1~~.1~~3~~.0~~3~~
2002-10~~01~~	SA3#25	SA3-020507 SA3-020508			~~Copyright date changed to 2002.~~Included relevant information as decided at SA3#24	0~~1~~.1~~3~~.0~~3~~	0~~1~~.2~~3~~.0~~4~~