ETSI TS 181 010 V1.1.1 (2005-06)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service requirements for end-to-end session control in multimedia networks (Release 1)

Reference

DTS/TISPAN-01013-NGN-R1

Keywords

multimedia, network, service

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

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/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://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 Specification (TS) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

Introduction

The present document provides general requirements for session control, to support and further develop the capabilities described in TS 181 014.

1 Scope

The present document provides a set of requirements for the session control service capability. The present document does not specify any particular requirement to the signalling protocol. However, it includes a list of general requirements that have to be considered when developing solutions to particular requirements.

2 Void

3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 180 000 (see Bibliography) and the following apply:

API	Application Programming Interface
BICC	Bearer Independant Call Control
ISUP	Integrated Service digital network User Part
NGN	Next Generation Network
SIP	Session Initiation Protocol

4 General requirements

4.1 Minimum session setup time

All the procedures and mechanisms should have a minimum impact on the session setup time as perceived by the user. When there is a choice between performing tasks at session establishment or in transactions prior to the session establishment, then the tasks should be performed prior to the session establishment. An example of such a task is user authentication.

4.2 Minimum support required in the terminal

As terminals could be rather small and "basic" devices, compliant terminals shall have a minimal capability set. Mandating support for features by the terminal shall meet this requirement. Should terminals have additional capabilities, this shall be made clear during sign-on.

4.3 Minimum trust put by the network in the terminal

As terminals are out of the control of a network operator, the trust put by the network in the terminal for proper functioning of the service shall be kept minimum.

Information provided by the terminal shall be labelled as user-provided, information provided by the network shall be labelled as network-provided. Processes using this information will then be able to make sound judgement on the validity of the information. E.g. session measurements provided by the terminal may be suspect in a dispute when there is different information available from the network on the same session.

4.4 Roaming and non-roaming scenarios

In case of nomadism, all the requirements must be met for both roaming and non-roaming scenarios. There should not be a significant change in the signalling procedures between roaming and non-roaming scenarios.

4.5 Access network independency

The network-based session control procedures shall be independent of the access network (and access network technology) where the user is located.

4.6 Internetworking

The services supported by the NGN session control shall be interoperable with other session control protocols (SIP, BICC, ISUP, H323, the 3GPP session control protocol, etc.). However, the requirements related to the support of end to end functionalities defined by these other session control protocols (e.g. overlap signalling in ISUP) with which interworking is desired are not presented in the present document.

NGN session control protocols must be able to encapsulate unique, optional or custom elements of the adapted session control, in order to enable complete session management by the providers session control applications.

The solution developed for a particular requirement expressed here shall not preclude the NGN control protocol to interwork with another profile of the same protocol. In order to fulfil this requirement, some control may be needed at the boundaries of the administrative domains controlled by the NGN control protocol.

The interworking between two administrative domains controlled by the NGN control protocol, shall be supported. In order to fulfil this requirement, some control may be needed at the boundaries of the administrative domain controlled by the NGN control protocol.

5 Signalling Path Requirements

5.1 Signalling route

The route of the call control signalling shall be hidden from the terminal. Therefore the terminal shall only know of the route to its Session Server. This session server may however act as a proxy to the real session server in the home network.

There may be a hot-standby session server, there may be a hot-standby session server proxy.

Terminals may be aware of a hot-standby for their sessions.

5.2 Session Server Routing

All signalling messages exchanged during a session initiated by the end user terminal (outgoing session) or during a session initiated toward the end user terminal (incoming session) must transit through the end user terminal's Access Session server, so that the services provided by the Access Session server can be delivered.

All signalling messages exchanged during either an outgoing session initiated by the end user terminal or an incoming session to the end user terminal must transit through the end user's Service call server, so that the Service call server can properly trigger the services allocated to that user.

5.3 Fraud containment

There shall be a way to prevent any malicious user from bypassing any network entity in the signalling path and still getting service.

6 Session control procedures

6.1 General requirement

An end user shall be able to request the establishment of a session with any other end user, of whom it knows the user Name E.164 number of other identifier as in use by the service provider.

An end user shall be able to request the termination or modification of any established sessions in which it takes part.

NOTE 1: The need for a permanently allocated "private" user identity assigned by the network to an end user, to which the end user does not have access is outside the scope of the present document. Such an identity could be used for purposes such as authentication, authorization, administration, and possibly charging and accounting.

NOTE 2: There may be limitations on the ability to modify certain aspects of a session due to billing for reserved resources, scheduling, available route capabilities, etc.

If it is desired to modify a session, and mid-session modification is impossible, there should be the option to immediately negotiate and establish a follow-on session with new session parameters.

6.2 Release of a session by the network

The network shall be able to initiate the release of a session of an end user terminal resulting in the release of all resources associated with it (e.g. in pre-paid calls when the user runs out of credit).

This may be done without involving any intervention from the terminal.

Such a request shall originate the release of all the network resources associated with the session of the end user terminal: bearer resources and signalling resources.

It shall be possible to notify other parties involved in the session, if any, of the termination of the session of the end user terminal.

6.3 Identities used for session establishment

6.3.1 Calling user identity

The identity of the calling user shall be provided.

It shall be possible, for the calling end user, to inform the called party of his user identity. On request of the originating user, the user identity may be withheld. There shall be users for which the user identity will never be withheld. Which parties these are, e.g. emergency services, is a matter of policy.

6.3.2 Called user identity

An end user terminal may be registered under a set of different user identities. As such, sessions destined to the user can be placed to any of the registered user identities. Certain filtering rules or services (done by the network or the called user terminal) may be based on the called user identity.

As such, it must be possible, for all sessions, to deliver the user identity used to reach the called party to network entities in the forward direction up to called party terminal.

It must also be possible, for all sessions, to deliver the user identity used to reach the called party to network entities in the backward direction up to calling party terminal. There shall be a way for the called end user to request any information related to his identity not to be divulgated to the calling end user or to any not-trusted network entity. Which mode is the default is a matter of policy.

6.3.3 Open service API

It shall be possible to bind third-party service notes to a session server for the purposes of providing service features over and above the basic service.

This binding may be performed during registration or possibly later.

These feature servers will be interrogated when the event they are registered for occurs.

End-users will have given permission explicitly (acceptance of terms of service for the particular feature) or implicitly (lawful interception) for the establishment of these bindings.

7 Bearer establishment

The session control protocol shall be used in conjunction with a media control protocol that describes the mono or multi media session.

Such a media control protocol may be encapsulated in the session control protocol (e.g. SDP and SIP) or invoked in parallel (e.g. H245 and H225).

During the session initiation request, the calling user terminal shall give the parameters of the media session it wants to establish.

The called user terminal shall have the possibility to participate in the media session parameters negotiation.

A terminal receiving a request to establish a media flow may reject the media flow based on its media parameters.

It shall be possible to offer multiple sets of media parameters for a particular media flow, the recipient may select one of these.

For NGN release 1 there is no requirement for a terminal of network entity to modify the parameters to engage in a negotiation. This may change in future releases.

7.1 Successful bearer establishment

Successful bearer establishment must include the completion of any required end-to-end QoS signalling, negotiation and resource allocation.

7.2 Network intervention

Both the access and the service call server shall have access to the requested media session parameters (e.g. for charging or resource management purposes).

The network shall have the possibility to participate in the media session parameters negotiation for the purposes of indicating that this session may or may not be supported by the network at this point in time.

Both the access and the service call server shall be able to deny the session establishment due to requested media session parameters.

In NGN release 1 it is not required to modify the media parameters for an established session. This may change post Release 1.

7.3 Independency between the session control protocol and QoS/Resource allocation

Resource allocation schemes must be independent of the selected session control protocol. This allows for independent evolution.

7.4 Correlation between the session control protocol and QoS/Resource allocation

A correlation shall be done between a dialog context in the control plane and, if existing, the resource requests originated by the end user terminal in the transport plane in order to ensure that an end user terminal which is requesting resource allocation has previously been authorized.

7.5 Resources allocation

In establishing a session, it must be possible for an application to request that the resources needed for bearer establishment are successfully allocated before the destination user is alerted.

7.6 Early media

Early media refers to media that is exchanged before a particular session is accepted by the called user (e.g. announcement). Support for early media is required.

8 Accounting

It shall be possible to account for session usage. The usage shall be reported containing session duration as well as session type, media flows supported (type and quality) and session participants.

9 Charging

On-line charging shall be possible. This means that the capability shall be able to generate appropriate accounting records in real-time. The means of (conveying) this charging is outside the scope of the present document.

10 Security requirements

10.1 Authentication

An end user shall be authenticated at registration time before the use of signalling resources is authorized.

The Service call server is responsible for authenticating the end user. As a consequence, the authentication method must be able to work when there are signalling entities (e.g. the Access call server) in the signalling path between the authenticator and the authenticated user.

The end-user shall not be able to use the services if they are not authenticated.

10.2 Message protection

Signalling entities (end user terminals and network entities) shall be able to communicate using integrity protection (ability to verify that the message has not been modified by a non authorized party) and replay protection.

Signalling entities (end user terminals and network entities) shall be able to communicate confidentially.

10.3 Delegation

It must be possible to perform an initial authentication of the end user based on long-term authentication credentials, followed by subsequent protected signalling that uses short-term authentication credentials, such as session keys initialized during initial authentication. The used authentication mechanism is able to provide such session keys.

It shall be possible to apply subsequent message protection as soon as possible, even during the initial authentication period.

The Service call server that performed the initial authentication must be able to securely delegate subsequent signalling protection (e.g., session keys for integrity or encryption) to the Access call server.

10.4 Establishment of mechanisms

A method must be provided to securely establish the security mechanisms to be used between the end user terminal and the Access call server.

10.5 Verification of messages

10.5.1 Verification at the Access call server

The Access call server must be able to guarantee the message origin and verify that the message has not been changed (e.g., it is integrity protected).

10.5.2 Verification at the Service call server

The Service call server needs to receive an indication if the Access call server was able to verify the message origin and whether it was integrity protected or not.

10.5.3 Confidentiality

Mechanisms shall exist so that messages may not be read by unauthorized third parties.

10.5.4 Prevention of denial of service

The risk of a call server to receive a denial of service attack shall be minimized. For instance, a malicious device could learn a call server IP address and port number and establish an attack to that call server.

10.5.5 Hiding requirement

The signalling messages that are sent between administrative domains shall reveal the least information possible about the underlying network configuration.

A network operator need not be required to reveal the internal network structure to another network.

A network operator need not be required to expose the explicit IP addresses of the nodes within the network (excluding firewalls and border gateways).

11 Emergency sessions

The establishment of an emergency session by a user shall be *technically* possible even if this user is not registered and not authenticated.

NOTE: Local regulations may prompt a service provider to disable this aspect and hence it shall be possible to disable this for all or particular groups of terminals.

12 Lawful interception

Sessions shall allow for lawful interception. Depending on the local regulations and the mandates given to the law enforcement officers the session meta-data and/or the media flows shall be available in real-time.

- Meta-data shall contain the presentation identities of the participants as well as the unique identifier of the user within the service provider, the terminal identities of all the participants of the session, the media flows opened as well as their end-point addresses. As well as the terminal locations shall be made available.

- The media content shall be provided at the handoff point as transported. If the service provider provides and encryption service (i.e. is aware of the encryption method and the keys) the media shall be offered decrypted.

Annex A (informative): Bibliography

- ETSI TS 122 228: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS); Stage 1".

- ETSI TS 181 014: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Services and Capabilities Requirements for TISPAN NGN Release 1".

- ETSI TR 180 000: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Terminology".

History

Document history		
V1.1.1	June 2005	Publication