3GPP TR 22.986 V11.0.0 (2012-09)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Service Specific Access Control (Release 11)

Keywords
Emergency, service, access

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.

Introduction

In an emergency situation, like Earthquake or Tsunami, degradation of quality of service may be experienced. Degradation in service availability and performance can be accepted in such situations, but mechanisms are desirable to minimize such degradation and maximize the efficiency of the remaining resources.

When Domain Specific Access Control (DSAC) mechanism was introduced for UMTS, the original motivation was to enable PS service continuation during congestion in CS Nodes in the case of major disaster like an Earthquake or a Tsunami.

In fact, the use case of DSAC in real UMTS deployment situation has been to apply access control separately on different types of services, such as voice and other packet-switched services.

For example, people's psychological behaviour is to make a voice call in emergency situations and it is not likely to change. Hence, a mechanism will be needed to separately restrict voice calls and other services.

As EPS is a PS-Domain only system, DSAC access control does not apply.
This SSAC TR identifies specific features useful when the network is subjected to decreased capacity and functionality. Considering the characteristics of voice and non-voice calls in EPS, requirements of the SSAC could be to restrict the voice calls and non-voice calls separately.

For a normal paid service there are QoS requirements. The provider can choose to shut down the service if the requirements cannot be met. In an emergency situation the most important thing is to keep communication channels uninterrupted, therefore the provider should preferably allow for a best effort (degradation of) service in preference to shutting the service down. During an emergency situation there should be a possibility for the service provider also to grant services, give extended credit to subscribers with accounts running empty. Under some circumstances (e.g. the terrorist attack in London on the 7 of July in 2005), overload access control may be invoked giving access only to authorities or a predefined set of users. It is up to national authorities to define and implement such schemes.

1 Scope

This Technical Report (TR) presents the results of the Study on Service Specific Access Control (SSAC). The intent of this Study is to assess the ability of 3GPP specifications to meet requirements identified for Services Specific Access Control. This Study considers the following aspects:

- Study use cases and clarify issues in SSAC in EPS.
- Describe the considerations and the problems with existing access control, which are identified in the use cases
- Identify candidate requirements and aspects for providing SSAC in EPS.

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 TR 23.898: "Access Class Barring and Overload Protection (ACBOP)"

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].

3.2 Symbols

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

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].

4 Use Cases

Use case 1

Japanese operators provide 'Disaster Message Board' services whenever a major disaster has happened such as an earthquake, tsunami or typhoon. This service enables the large number of subscribers to access the message board in order to post or retrieve information concerning the safety of individuals in the affected area with their mobile phones during a major disaster.

The human psychological behaviour is to make a voice call in emergency situations. Thus increased voice traffic consumes too much bandwidth for accessing other services such as the Disaster Message Board and/or data services (e.g. SMS).

Hence, a limiting mechanism is required to differentiate bandwidth consuming real-time services (e.g. Voice) from bandwidth-efficient data service to access to e.g. a Disaster Message Board.

Use case 2

As described in the Use case 1 above, subscribers may wish to make voice calls to check on the safety of individuals and it may cause congestion. Under such a situation, prioritised subscribers (e.g. governmental, military civil authorities) and (depending on national regulation) access to emergency services should still be allowed access to EPS, while voice calls for other subscribers are restricted.

5 Considerations

In UMTS, Domain Specific Access Control (DSAC) has been introduced. According to Section 4.1.1 of TR23.898 [x], the original motivation was to enable PS service continuation during congestion in CS nodes.

Although that was the original motivation, operators have been using DSAC to restrict CS calls while permitting PS sessions. Operators want to avoid service discontinuity in the packet data services due to the congestion in the voice calls side. Consequently, the use case of DSAC in a real deployment situation has been to apply access control separately on different types of services, such as voice and other packet-switched services.

The voice services will be provided by MMTeL using IMS in EPS; however the VoIP will be used in the same way as the existing CS-domain voice services (e.g. including Emergency Calls). This means customer experience per "Service" in EPS is not different from UMTS.

It is reasonable that DSAC principles are to be applied in the PS-domain only EPS as well. However, EPS is a PS-Domain only system, so the "Domain Specific" way of access control cannot be applied as it is now. Hence, "Service Specific" Access Control (SSAC) has to be specified and introduced to EPS.

6 Candidate Requirements

The following is the principle for the Service Specific Access Control.

1. The EPS shall provide a capability to apply independent access control for telephony services (MMTEL) and other data services, for mobile originating session requests from idle-mode.
2. The EPS shall provide a capability to assign a service probability factor for each of MMTEL voice and MMTEL video:
   - assign a barring rate (percentage) commonly applicable for Access Classes 0-9;

   - assign a flag barring status (barred /unbarred) for each Access Class in the range 11-15.

   SSAC shall not apply to Access Class 10.

3. The SSAC shall be provided by the VPLMN based on operator policy without accessing the HPLMN.
4. The SSAC shall provide mechanisms to minimize service availability degradation (i.e. radio resource shortage) due to the mass simultaneous mobile originating session requests and maximize the availability of the wireless access resources for non-barred services.

7 Conclusion

This Technical Report (TR) on Study on Service Specific Access Control (SSAC) identified the requirements for SSAC and considered the following aspects:

- Use cases were documented and issues clarified for SSAC in EPS.
- Considerations were described as well as problems with existing access control, which are identified in the use cases.
- Candidate requirements and aspects were identified for providing SSAC in EPS.

From this study, it is concluded the following:

- EPS is a PS-Domain only system, so the "Domain Specific" way of access control cannot be applied as it is now. Hence, "Service Specific" Access Control (SSAC) has to be specified and introduced to EPS.

  SSAC shall provide mechanisms to minimize service availability degradation (i.e. radio resource shortage) due to the mass simultaneous mobile originating session requests and maximize the availability of the wireless access resources for non-barred services.

It is also concluded that the content of this TR be used as a basis for further work within 3GPP.

Annex A:
Change history

Change history											
TSG SA#	SA Doc.	SA1 Doc	Spec	CR	Rev	Rel	Cat	Subject/Comment	Old	New	WI
SP-42	SP-080786	S1-084390	22.986	-	-	Rel-9	-	One-step-approved at SA#42	1.0.0	9.0.0	SSAC
2011-03	-	-	-	-	-	-	-	Update to Rel-10 version (MCC)	9.0.0	10.0.0	
2012-09	-	-	-	-	-	-	-	Updated to Rel-11 by MCC	10.0.0	11.0.0	