Report 23 ITS Technical Report

Handläggande organ

ITS, Informationstekniska standardiseringen

Fastställd 2006-05-15

Utgåva 1.0

Sida 1 (28)

Aspects of Developing Support for the International Emergency Preference Scheme (IEPS) in Swedish Public Communications Networks - TECHNICAL REPORT

The technical report contains an overview of consequences related to a future national support of the *International Emergency Preference Scheme* (IEPS) in both public land mobile networks (PLMN) and public switched telephone networks (PSTN/ISDN). The report also contains a description of priority services in evolving Next Generation Networks (NGN) in relation to IEPS.

Contents

1 Introduction

The *International Emergency Preference Scheme* (IEPS) is an international priority service for the use of public telecommunications by national authorities for emergency and disaster relief operations. IEPS is designed to give these authorities preferential treatment in crises and other situations where there is an increased demand for telecommunications or the International Telephone Service may be restricted due to damage, reduced capacity, congestion or faults.

In Sweden, there is an ongoing effort related to the introduction of priority services for both fixed and mobile telecommunications networks. This report outlines the necessary steps needed to extend a national priority service to also include support for existing and evolving standards related to IEPS. When a future need for a national IEPS support has been identified, the consequences presented here is intended to serve as a starting point for such an extension.

2 Scope

This technical report is primarily related to the facilitation of IEPS support in national networks giving priority to voice calls between international communications networks. IEPS extensions related to multi-media are not within the scope of the technical report although the majority of conclusions remain valid.

In the discussion of IEPS features related to security, routing or network management, these features complement the inherent resilience that each operator has built into the design, maintenance and operation of their respective network or networks[1]. Priority services should therefore be regarded as a complement to this inherent resilience for use in special situations. In the discussion of security below, the measures under discussion are also additions to existing security features.

3 Priority Services in Telecommunications Networks

The evolution of priority services has taken place in two stages. Before the digitization of network technology several countries including Sweden had priority services with varying scope and functionality. During the last decade or so, selected countries have introduced more modern services where a number of mechanisms are used to increase the likelihood for call-completion for authorized users. Several other countries are also considering the introduction of similar services. A natural consequence of these efforts is to connect national priority services to improve the resilience of cross-border communication services.

3.1 Technical Features in Priority Services

There are several technical features that can conceivably be used to reduce the effects of congestion, failures and faults in telecommunication networks. Priority services utilize a number of different components whose functions can be divided into categories:

- Exemption from restrictive network management controls
- Preferential access to network resources
- Routing enhancements

[1] The underlying reliance on power is left outside the discussion.

- Security features where authentication and authorization are major components

3.1.1 Exemption from restrictive network management controls

Modern telecommunications networks are equipped with a number of sophisticated controls that alter the flow of traffic with the aim to enable as many calls as possible to be completed. These controls can be applied both manually and by automatic, software controlled invocation to minimize the consequences of abnormal increases in traffic demand, congestion in connected networks, failures of international or national exchanges or failures of international or national transmission systems. The entities to which network management controls can be applied range from circuit groups to intelligent network nodes. One type of network management control is call-gapping, which sets an upper limit on the output rate of calls that are allowed to be routed to a destination. One other example is line load control where users are placed in two or more categories. By invoking line load control, calls from (rather than to) one or more of these categories are not accepted.

3.1.2 Preferential access to network resources

There are two primary mechanisms that can be used to give priority calls preferential access: precedence and pre-emption. Precedence means that priority calls are placed in queues and are given access to available resources before ordinary calls, whereas pre-emption includes actions where resources are freed and the released capacity is then assigned to the priority call. The queuing and pre-emption capabilities should extend to as many network elements as possible. As many users in need of priority services are affected by PBX or Centrex facilities, it is desirable to ensure that queuing and pre-emption can be extended into these environments.

3.1.3 Routing enhancements

The routing of calls is one important factor affecting the resilience of telecommunications networks. Bearing in mind that the need for priority stems from network restrictions caused by damage, reduced capacity, congestion or faults, it is desirable to route priority calls in such a manner that call-completion rates are maximized. Such routing enhancements could conceivably be different from those that are used to route normal calls even though each operator has designed the network with an appropriate amount of resilience from a commercial perspective. If one network for example experienced congestion or network damages, priority calls could be transferred to another operator's network and forwarded around the damaged or congested part making it possible to complete the call.

Even though traffic routing methods in circuit -switched networks can be categorized into four basic categories ([10]), fixed routing (FR), time-dependent routing (TDR), state-dependent routing (SDR), and event-dependent routing (EDR), there can still be differences between each operator's implementation and operational use. Interworking thus becomes an issue to consider in any attempt to introduce more sophisticated routing methods than those that are available in each network.

3.1.4 Security features

Priority services can potentially cause disruptions to normal network operations, in particular if certain priority calls are given the right to pre-empt ongoing calls or calls undergoing set-up. A priority service must therefore contain authentication and authorization mechanisms together with other network security measures to minimize the risks of corruption of, or unauthorized access to network traffic and control. For priority services there are two primary authentication and authorization methods: terminal based and IN-based solutions. In an IN-based solution, there is a design choice to be made if the service user shall receive priority treatment in the parts of a network preceding the authentication and authorization process in a network node. Again, this design choice is of particular importance for priority services that include pre-emption.

There is one further security aspect that is important to consider. The traffic and location information that can be obtained from support and billing systems can be considered as being sensitive considering the intended user group. Ideally, access to this information should be restricted. Within this context, the large amount of data that is collected during normal operation can be regarded as an inherent security feature.

3.2 Main Standards for Priority Services

The development and implementation of standardized solutions for wireline and wireless networks supporting priority features varies. For wireline networks, Multi-Level Precedence and Pre-emption (MLPP, [18]) contains several IEPS related features. MLPP has also several drawbacks, principally related to the lack of authentication that has restricted the application of MLPP to private networks. The priority service standard [17] also contains usable features but is lacking authentication procedures and requires activation which in many cases is unwanted. In GSM networks, the enhanced Multi-Level Precedence and Pre-emption (eMLPP, [19]) together with access classes ([21]) contain several useful features. Together, they provide selected users priority network access[2], queuing and pre-emptive mechanisms using SIM-based[3] authentication. The configurable support for pre-emption means that priority calls can force the release of network resources from ongoing non-priority calls. In 3G networks, there is currently a lack of vendor support for eMLPP.

At the moment wireless networks has to be considered as the primary candidate for the introduction of priority services. The ongoing development of and migration to new network architectures will improve the situation for wireline networks as described in section 7 below. It should be noted that a priority service where only access classes are used is not a platform for the development of IEPS support.

3.3 International Examples

The international interest for priority services is increasing, and in the light of recent events it is likely that several nations will actually implement new priority services within the next years. Below, we describe relevant, existing priority services.

3.3.1 Priority Services within the USA

In the United States, work on priority services has been and continues to be a long-term collaborative effort between operators, vendors and authorities. The Government Emergency Telecommunications Service (GETS), a priority service for wireline networks, has been operational for a number of years. GETS relies on several technical features that together make up for the absolute majority of the IEPS features that are considered as essential and optional as described in [1]. GETS as such does not contain pre-emption as a basic feature.

During the last years, Wireless Priority Service (WPS) has been implemented in a staged process where an initial capability was introduced in 2002 using

---

[2] Subject to operators' actions.

[3] Subscriber Identity Module

access classes and eMLPP. This capability was then extended in several ways:

- Queuing mechanisms to ensure that the general public is granted a suitable percentage of network resources
- Exemption from restrictive network management controls[4]
- Simplifications to WPS service invocation

WPS does not contain pre-emption. Together, GETS and WPS can be considered as the most complete examples of operational priority services in public networks. It is also evident that the technical features that make up GETS and WPS have influenced the work on IEPS within ITU.

3.3.2 Priority Services within Canada

Canada has introduced priority services in both their wireline and wireless networks. The development and introduction of priority service in GSM-based networks have been based on WPS. In the wireline case, the network management control mechanism line load control is combined with data bases where essential and authorized users can register numbers that should be given priority access to dialing (PAD). When applied, PAD permits dialing (originating a telephone call) from a phone that has been identified as essential.

3.3.3 Priority Services within the United Kingdom

The primary priority service within the UK is Access Overload Control (ACCOLC). ACCOLC is a government-authorized service based on GSM standards ([21]) to restrict access to signaling channels for certain mobile terminals based on the SIM-card. By separating normal users from priority users, an operator can initiate actions to restrict parts or the whole user group to free resources for priority calls. During the events in London, ACCOLC was activated in one operator's network within a 1 km radius heavily congested by an excess number of call attempts ([D1]).

In the UK, there is also ongoing work in developing a priority service within a next generation network setting as described in [D2].

3.4 Organizational Structure

Priority services should not solely be seen as a set of technical functions that are designed to give selected users preferential access to network resources. The primary aspect of a priority service beside these technical features is the organizations that in some capacity are involved operating the service. The primary actors in this setting are[5]:

- Principal Service Customer
- Authorization Agency
- Service Provider
- Service User
- Network Operator
- Networks

Relevant aspects for the relationships between these entities will be described from Figure 1 below.

---

[4] Compare with the discussion in section 3.1.1.

[5] Here, we follow the ITU-T M.3550 standard with some national deviations.

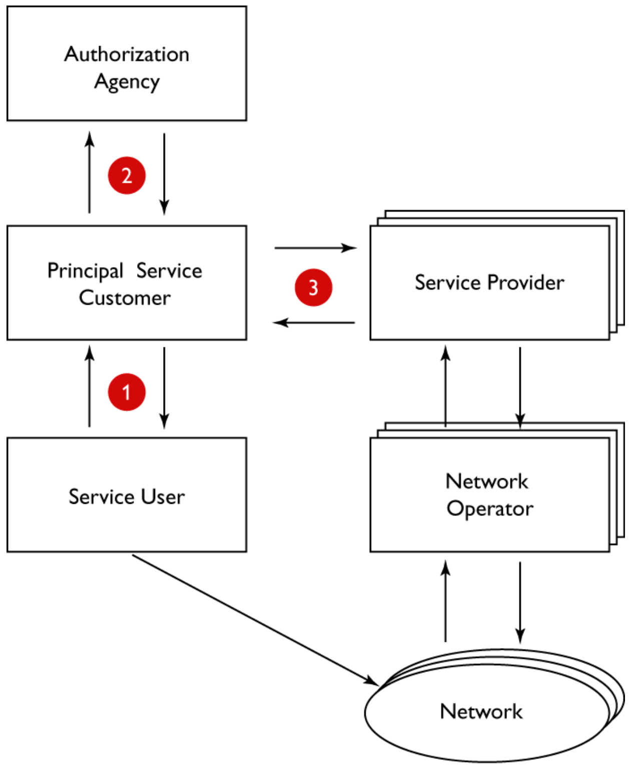

Figure 1 Interaction between entities involved in providing a priority service.

A user who has a identified a need for access to a priority service, sends an application to the principal service customer (PSC) who passes the request to an agency with two primary responsibilities: defining criteria for determining which potential users should be given access to the priority service and applying these criteria as request are made. The PSC has several responsibilities. One such responsibility is the negotiation of service level agreements (SLA) with the service providers. These SLAs are more likely to contain information related to the technical features that should be given to an authorized user, rather than a set of strict quality of service parameters. The interaction between the PSC and the service providers would also include an ongoing discussion regarding the maintenance and evolution of an existing priority service. In the description of IEPS service management below, we will use the model presented here as a starting point for an analysis of national consequences.

4 Description of the International Emergency Preference Scheme

IEPS is designed to significantly increase the ability of IEPS users to initiate and complete voice and (voice-band) data communications via PSTN, ISDN or PLMN irrespective of their bearer technology. The technical features that each country chooses to make up for a national priority service can either be permanently enabled or activated through special procedures with similar implications for an IEPS capability.

This section starts with a brief description of features and standards within the first phase of IEPS standards. Recent work related to the extension of IEPS is then described. It is important to note that public access to emergency services is not addressed as a part of IEPS.

4.1 IEPS Standards and Features

The development of IEPS capabilities has taken place within the International Telecommunications Union, ITU, and has to a great extent been affected by existing priority services. The primary IEPS standard ([1]) describes rather than specifies the particular mechanisms that are to be used to ensure preferential treatment. Instead, a number of the features presented earlier in section 3.1 can be used where each country is to decide on the best use of these depending on national requirements and conditions. The features that are deemed to be essential features relate to:

- Priority dial tone
- Priority call setup message through signaling network
- Priority indicator in bearer networks
- Exemption from restrictive network management controls

The main IEPS standard also describes a number of features that are deemed to be optional rather than essential. Examples of such optional features are routing enhancements and prescribed interactions with other services. It also does not describe the way a user should invoke IEPS on a call-by-call basis. Moreover, the main IEPS standard states that it is necessary to make arrangements with non-intermediate service providers of transit networks to transfer and act on call marking. The implications of this statement will be analyzed in section 5.1 below. ETSI later endorsed ([2]) the corresponding ITU-T Amendments (2002) to Q.761 – Q.764 ([13]-[16]) with few significant changes.

4.2 Recent Extensions to IEPS

Further extensions ([6], [9]) to the earlier IEPS standards were presented to the ITU-T for consideration under the traditional approval process during the beginning of 2006 and later accepted. The extensions are primarily related to the addition of parameters that can be utilized for IEPS calls using a number of different protocols as seen in table 1 below.

Table 1 Summary of protocol extensions related to IEPS.

Amends	Description of extension
ITU-T Q.761	Comments on ISUP enhancements related to IEPS
ITU-T Q.762	ISUP parameter additions related to IEPS
ITU-T Q.763	Addition to ISUP User Part formats and codes related to IEPS
ITU-T Q.764	Addition to ISUP User Part signaling procedures related to IEPS
ITU-T Q.1902.1	Comments on BICC enhancements related to IEPS
ITU-T Q.1902.2	BICC parameter additions related to IEPS
ITU-T Q.1902.3	Addition of BICC and ISDN User Part formats and codes related to IEPS
ITU-T Q.1902.4	Addition to BICC basic call procedures related to IEPS
ITU-T Q.1950	Additions to Bearer independent call bearer control protocol related to IEPS
ITU-T Q.2931	Amendment to Digital Subscriber Signaling System No. 2 for basic call and connection control related to IEPS
ITU-T Q.2630.3	Amendment to AAL Type 2 Signaling Protocol

The national work on priority services have entirely been directed towards establishing support in GSM- and UMTS-based mobile networks as well as the ISUP-based PSTN since these networks are the major networks used to complete national voice calls. The comments below are therefore restricted to the Q.7-series amendments. These amendments should be considered as a whole rather than as separate additions that can be supported individually or not.

The amendment to Q.761 states that the implementation of IEPS support can be made in a phased approach:

- The minimum implementation is for national networks to support IEPS call marking in the forward direction. Calls with this marking should then bypass any restrictive call handling procedure at international gateways.
- Improvements on the basis capability can be to enable the generation of an early Address Complete Message (ACM) to reduce the risk of call set-up failures due to timer expiration on congested trunks.
- Further improvement of IEPS support can be realized regarding priority levels and identification.

The related amendments to Q.762 and Q.763 stipulate the addition of IEPS call information field identifying the country or the international network pertaining to IEPS call origination as well as an indication of the national priority level of an IEPS call. This national priority level, a 5-bit field thus providing 31 priority levels, is subject to bilateral agreements.

5 National Consequences for the Development of IEPS Support

The development of a future national support for IEPS involves a number of changes, both on technical and organizational levels. IEPS calls are by definition international calls and therefore often affect two or more separate but interconnected networks that can be owned and operated by different entities.

This section starts with an analysis of how international transit networks can be handled during the development of national IEPS support. We then comment on service management aspects to reflect what procedures between operators and authorities that are needed to operate an IEPS service. In section 5.3, the national work on priority services is related to essential and optional IEPS features which is followed by an analysis of the consequences of defining a subset of national priority users that are to be entitled to make IEPS calls. Concluding the section is an analysis if security aspects. The findings in this section are the basis for the recommendations in section 8 and the proposed IEPS implementation plan.

5.1 Handling of Transit Networks

IEPS will in many cases involve international carrier networks to transfer and act on call marking related to IEPS calls. In our analysis of IEPS driven changes, we primarily consider two types of IEPS calls:

- IEPS calls originated within a national network that shall be given priority *to* the appropriate international gateway
- IEPS calls originated outside Sweden to a subscriber within the national network that shall be given priority *from* the appropriate international gateway

Here, we take the view that any two nations that want to enter a mutual agreement regarding IEPS calls has to analyze exactly what networks (outside the originating and destination network) are involved in the exchange of calls and then make suitable arrangements with the corresponding service-providers. It should be noted that for these service-providers, it is not certain that per-call precedence will be given since the priority call-marking is not easily available and acted on. In most cases, the time it takes to identify a packet with priority marking is longer than the normal queuing time in routers or gateways. In the same way, pre-emption might not always be an option.

The introduction of priority services can potentially have legal implications depending on the way the service is introduced. One way is to mandate operators by law to provide a national priority service. In an IEPS setting, there is an inherent difficulty since international carriers can be affected by several national legislations. It is therefore likely that service level agreements with the carriers rather than legal requirements are the best approach for introducing IEPS support in carrier networks. The legal option is probably only viable if IEPS becomes a pan-European requirement. The minimal requirement is that international carriers should preserve IEPS signaling to ensure that priority calls can be given preferential treatment in the destination network.

5.2 IEPS Service Introduction and Management

Starting from the organizational structure in section 3.4, the management of an IEPS service involves three entities:

- Principal Service Customer
- Authorization Agency
- Service Provider

Their respective responsibilities are likely to vary during the introduction of the service as described below.

The pre-implementation planning has three main components: technical planning, administrative planning and service level agreements. Technical planning, involving both the principal service customers and the involved service providers, would include the investigation of the capabilities of involved carrier networks with an emphasis on priority features and resilience. The principal technical decision to make is if special routing arrangements for IEPS calls should be applied or not. These routing arrangements could be based on resilience rather than cost. The administrative planning involving the authorization agencies as well as the PSCs relates to an investigation of the criteria each of the countries are willing to apply for IEPS service access, which should be used as a basis for service level agreements between the two countries principal service customers. These SLAs would also contain information detailing the priority features that should be applied to each IEPS call within the involved national priority schemes, and the traffic pricing policies rather than subscription policies that should be applied.

The outcome of the pre-implementation planning is service level agreements between the PSCs outlining the technical features and the mapping of priority levels that should be used to exchange priority calls, and the corresponding agreements between the national PSCs and SPs.

Technical implementation is the responsibility of the individual SPs followed by service tests involving both the respective PSCs and SPs. Similarly, the long term evolution of the IEPS service is likely to be a joint undertaking between the same entities with the PSCs sharing the primary responsibility.

5.3 Comparison of IEPS Features and National Work on Priority Services

The National Post and Telecom Agency, PTS, have been working on analyzing technical, financial and organizational consequences of introducing priority services in both wireline and wireless public telecommunications networks. One aspect of this work has been related to determining national needs resulting in requirements. Operators and their suppliers have then been tasked to investigate the possibilities of introducing services satisfying the users' needs. During the course of this work, tests of priority services have also been made. In the following sections, we compare aspects of this work in relation to the technical features of priority services described in section 3.1 above.

5.3.1 Exemption from restrictive network management controls

Exemption from restrictive network management controls (RNMC) can be implemented on several levels. A low-level exemption can be achieved by assigning suitable values to the Sub Service Field (SSF) in the Service Information Octet (SIO) in accordance with [7]. This marking would ensure that signaling traffic for priority calls would be placed in queues on congested links and not be exposed to RNMCs at the MTP level. The introduction of such a feature in existing circuit-switched wireline networks is a considerable undertaking. The value of such an undertaking has to be measured against the available signaling resources and other measures that are in place in current national wireline and wireless networks. The ongoing network changes that are described in more detail in section 7 should also be considered in this regard.

A more feasible solution to exempt priority calls from RNMC as specified in [12] is to modify the corresponding technical functions so that they are not applied to calls with a proper marking. In wireless networks, the eMLPP standard ([19]) does not contain this feature. It should also be noted that, according to the standard, there is a risk that calls with precedence can be released by pre-emptive calls.

The conclusion is therefore that it is unlikely that a national priority service will contain this feature in the short term. The introduction of such a feature for IEPS is in a sense a more limited undertaking, where changes need only to be applied to international gateways.

5.3.2 Preferential access to network resources

Priority dial tone for wireless connections can be considered as a part of access classes ([21]) where selected users are exempted from certain network management controls and therefore given an increased likelihood of successful call setup. Together with the eMLPP queuing and pre-emption capabilities, the priority service that has been considered contains several technical features that give selected users preferential access to network resources. In this context, roaming where subscribers are allowed to utilize all available networks to initiate calls can also be seen as one component in this regard.

For wireline connections, an earlier national priority service was based on access denial systems where only selected users were given dial tone in certain situations. In the course of the national work, the introduction of this feature or more sophisticated means (cf. PDA in section 3.3.3) of ensuring dial tone for authorized users on a line-by-line basis were not considered as a viable alternative. Instead, user organizations are encouraged to work together with their respective operator to ensure that enough resources are available. As such, this type of mechanism should be considered as an exemption to a restrictive network management control.

Marking of setup messages are used to give preferential treatment of priority calls during call setup. The national work has essentially been focused on two principles: precedence and pre-emption. Here, Sweden is an exception since most if not all of the priority services that are operational in public networks do not contain pre-emption. The desired capability is that no priority call shall be released after set up, which means that a priority indicator has to be dynamically assigned to each circuit and be maintained for the duration of the call.

Technical investigations show that it is possible to provide a wireline priority service that gives preferential access to network resources form the first local exchange extending to the called subscriber. As described in section 3.2, the main problem is that such a solution would have to be introduced as a national adaptation to existing technical systems rather than based on international standards. It is also likely that the development of support for the recent IEPS extensions will be made for products related to emerging next generation networks rather than their circuit-switched equivalents. During the course of the work on priority services, the treatment of priority within PBX and Centrex environments has also been considered. The conclusion here has been that the inclusion of priority services inside such environments has to be seen as a long term effort.

5.3.3 Routing enhancements

As part of the functional requirements that has formed the basis for the recent national work, routing enhancements have been included. These routing enhancements essentially contain three components: the invocation of a priority service in all available networks, the use of several operators' networks to route calls during set-up, and similar procedures to protect ongoing calls. The enhancements complement the mechanisms that each operator has used to design routing within their individual networks.

Of these alternatives, the third option can not be regarded as a viable option without fundamental technical and operational changes to existing and planned networks. In the wireless case, the first alternative can be implemented through roaming agreements with few technical consequences. The second alternative is also associated with considerable difficulties. The routing enhancements that have been utilized for GETS rely on the market subdivision between long-distance and local operators. In interconnection points at the originating side, calls can in succession try three long-distance carrier networks to increase the likelihood of successful call-setup. In Sweden, there is no similar subdivision where interconnection points can be identified and used to easily implement improved routing mechanisms. In this regard, topology hiding mechanisms like global title translation is one further complication.

At the moment, it seems unlikely that a national priority service established in current circuit-switched networks will contain routing enhancements for priority calls as compared to normal calls which obvious consequences for the short-term development of IEPS support. In the longer term, routing enhancements for coming packet-switched networks can be a more feasible option.

5.3.4 Security features

The principal security features that have been discussed within the national work are related to authentication and authorization (AA) on one hand, and the protection of call and location information on the other. For wireless networks, the primary AA mechanisms are those as provided by the eMLPP standard. For wireline networks the focus has been on developing AA mechanisms using IN functionality where both a distributed and a centralized architecture has been considered. In the centralized case, all operators would direct priority calls to one IN-node[6] where authentication and authorization would be performed. In the decentralized case, each operator would be responsible for either operating their own IN-based solution or procuring such a solution using a set of requirements determining capacity and resilience aspects. In both cases, the assumption has been that authentication and authorization only takes place in one network rather than every network that a priority call might traverse. The use of such a procedure, built on trusted networks, is particularly important to consider in an IEPS setting.

In the national work, two primary requirements have been formulated regarding the safeguarding of information related to priority calls and users. The basic requirement is the Electronic Communications Act ([D7]) that states that service providers supplying a basic communications service are obliged to protect information using appropriate means, a requirement that also provides a certain level of protection for priority users. The next level of information protection relates to the Security Protection Act ([D8]). There are today only a limited number of operators that support this more stringent requirement.

In the near term, an IEPS service primary security feature[7] is likely going to be based on the authentication and authorization methods described above. Enhanced protection of user data has to be considered as an item for further study.

---

[6] Redundancy and the provisioning of signaling links are left outside this discussion.

[7] As stated in section 2, other mechanisms, apart from the authentication and authorization of priority users, used by operators to protect the integrity of their networks are not considered here.

5.4 IEPS User Group Restrictions

In a national wireline priority service, IN-functionality is the likely candidate to process requests for service invocation. The IEPS standard is open to the possibility that not all users authorized to use the national priority service are necessarily entitled to use IEPS. An IN-based authentication solution can with few modifications be extended to accommodate such a procedure by performing a called number-analysis. International calls from users not authorized to use IEPS could, based on number analysis and stored information as shown in table 2 below, be rejected.

Table 2 Example information needed to impose restrictions on the national user group that should be authorized to perform IEPS calls.

Stored information	Comment
Access to national calls with precedence	–
Access to national calls with pre-emption	It is possible to restrict the number of people that should be granted the right to invoke pre-emption in a national priority service.
International call with precedence	The IEPS standard states that pre-emption in public networks should *not* be provided so that all IEPS calls shall be of the same class. Nevertheless, if two countries have multi-level priority service agreements for the mapping priority levels can be made between the parties. The security implications of supporting pre-emption are the strongest arguments *against* allowing pre-emption in a bilateral agreement.
International call: pre-emption	

The problem of restricting the number of people within an eMLPP-based wireless priority service that are entitled to invoke IEPS is not as straightforward. The standard does not contain any mechanisms that analyze the called number and depending on the country of destination decides to either use or not use the technical features within the standard. One partial solution would be to use priority levels in accordance with table 3 below.

Table 3 A possible service composition in a eMLPP-based priority service where only a selected number of users can invoke IEPS as shown below has a drawback in that IEPS calls could pre-empt national calls made using pre-emption. Interchanging the priority level would only mean that IEPS call could be pre-empted by national call made using pre-emption.

Priority level	**User**
0	User within the priority service with rights to invoke IEPS on international calls
1	User within the priority service with rights to invoke pre-emption
2	User within the priority service with rights to invoke precedence

To only give certain authorized users within an eMLPP-based national priority service access to IEPS therefore requires special procedures, for example in international gateways, which are outside the scope of current standard. These and other interworking procedures, in the form of call marking, marking interpretation and processing arrangements, have to be specified and agreed on in gateway points.

5.5 Additional IEPS Security Aspects

A priority service in general contains mechanisms that can potentially disrupt or otherwise harm network operation. These mechanisms are primarily related to the unauthorized injection of priority calls that are either given preferential access to available network resources or release resources using pre-emption thus preventing ordinary calls from being completed. In an IEPS setting, the possible security implications are of particular importance since national networks are potentially being exposed to a larger number of malicious users. It is therefore advisable to include two further mechanisms:

- The continuous monitoring of incoming and outgoing priority calls at international gateways
- The possibility to dynamically change the mapping of incoming and outgoing priority calls to different priority levels

This recommendation is of particular importance if pre-emption shall be supported in an IEPS setting. These two measures can together alleviate the most pressing security concerns by establishing technical systems and procedures for detecting and mitigating the most serious security breaches.

6 Strategies for Implementing IEPS Support

There are basically two strategies for implementing IEPS support. The first strategy, called IEPS Service Addition, is the addition of IEPS as a new service so that the IEPS priority indicator is generated in a network of the call originating country. Here, the IEPS priority indicator is set independently from any other indicator or condition and is included in the very first signaling message of the call set up procedure, e.g., IAM. The other strategy, called IEPS Service Extension, relies on an existing priority service which is extended at international gateway exchanges by a mapping of priority level indications to and from national priority levels required and applied in the terminating countries.

Below, we comment on the advantages and disadvantages using these strategies.

6.1 IEPS Service Addition

IEPS service addition can essentially be seen as the introduction of a new national priority service that is running in parallel with an existing service. One possible benefit of such a procedure is that changes to the composition of technical features used for one service would not necessarily affect the other service. One such change could be special routing of IEPS calls to one particular international carrier who is deemed to offer the most resilient international carrier service. This statement relies on the particular implementation of priority services, depending on if the two services are built on separate logical functions or if the same logical function can be initiated using both national and IEPS signaling parameters.

There are several principal drawbacks associated to this solution. One such drawback is that service addition is likely to require vendor support on a different level as compared to service extension, indicating a longer time before users can benefit from IEPS functionality. The number of IEPS service invocations is also likely to be quite low, which means that faults or malfunctions to a rarely used system are more likely to remain undetected or require more frequent testing arrangements.

6.2 IEPS Service Extensions

The principal advantage of introducing IEPS support by a mapping procedure is the envisioned shorter time until IEPS support can be realized. For example, if both the Swedish and Norwegian implementations of priority services in mobile networks would be based on eMLPP and use precedence, pre-emption or both in the same manner, (limited) IEPS support could conceivably be introduced by only requiring that carrier networks to maintain the associated signaling parameters. By introducing logical functions to exempt these calls from restrictive network management controls, a capable IEPS service could be introduced with relatively little effort.

The final choice between IEPS service addition and extension depends on the time scale. In the longer term, service addition is the more appealing alternative if the corresponding international standards and subsequent implementations are made.

7 Support for IEPS in Future Packet-Based Networks

Telecommunications networks of today are undergoing changes with a migration of previous circuit-switched networks to new network architectures with packet-based transport technologies. This migration is already in progress and is set to affect any implementation of IEPS or any other priority service that is implemented in a circuit-switched setting.

In this section, a set of network architectures and protocols relevant for IEPS and related priority services are described that are currently being developed in international standards bodies. The emphasis is placed on aspects related to the evolution of traditional operator's networks in general and ETSI's first release of next generation networks (NGN) standards in particular complemented by selected 3GPP and ITU-T initiatives. Internet-based, best-effort communications services are not treated.

7.1 Next Generation Networks: Architecture and Relevant Subsystems

The primary driver behind the development of architectures, protocols and systems for next generation networks (NGN) is the creation of unified service delivery architectures. To this end, key international standards organizations are working on creating suitable standards for both wireline and wireless networks as well as those converged networks with common cores and control planes but heterogeneous access environments. Within this work the IP Multimedia Subsystem (IMS) has gained almost universal acceptance as the common architectural and logical framework. At the end of 2005, ETSI published the first set of standards related to NGN. The primary goals ([3]) were:

- Enabling delivery of the services supported in a 3GPP IMS to broadband fixed lines
- Enabling PSTN/ISDN replacement (in whole or in part).

Several of the primary IMS extensions have implications for priority services as seen in Table 4 below.

Table 4 Key NGN extensions to the IMS network with corresponding implications for priority services.

Extension	Relevance for priority services
Control of access networks (QoS, admission control, authentication, etc.)	See section 7.2 below.
The interworking and interoperability with legacy networks	If a national priority service is implemented in existing circuit-switched networks, interworking with NGN is vital to ensure interoperability between legacy and evolving services. The interworking principles will require national standardization.
The co-ordination of multiple control sub-systems to a single core transport for resource control	See section 7.2 below.
Mutual de-coupling of the application layer from the session/call control layer and the transport layer	The de-coupling of the session/call control and transport layers could conceivably mean that not all elements of the transport layer are controlled by the session/call control layer to the same extent as in today's circuit-switched environment. One possible result is that routing enhancements for priority calls could become more challenging.

The NGN architecture is based on the re-use of the 3GPP IMS for SIP-controlled services including the control and delivery of real-time conversational services (SIP-based control). The 3GPP IMS is also extended to support additional access network types, such as xDSL and WLAN.

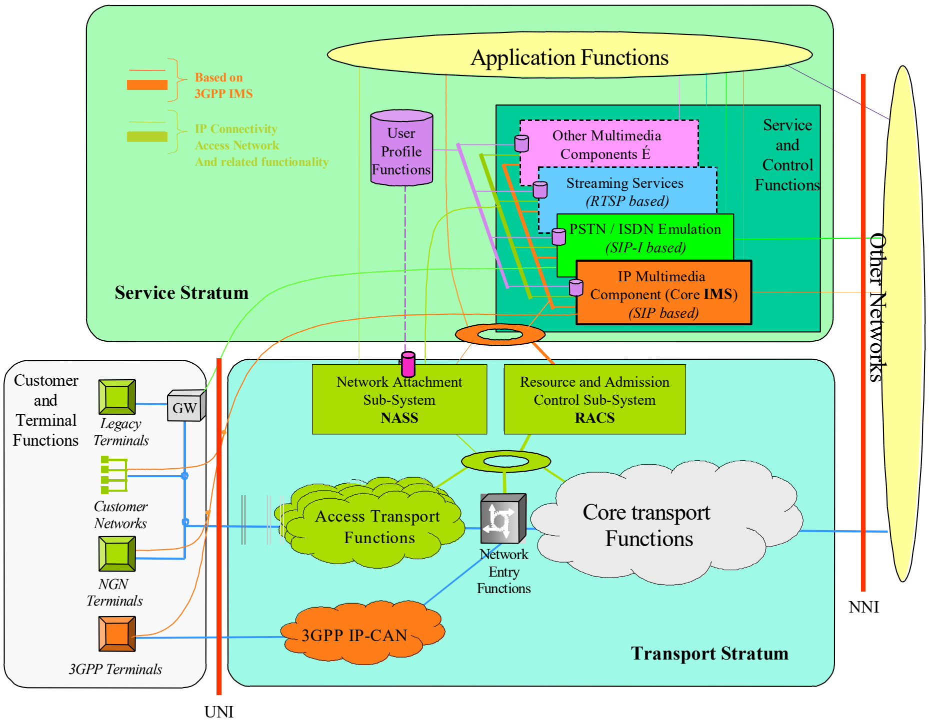

Figure 2 Overview of NGN component ([3]).

For priority services, the primary subsystem of interest is the Resource and Admission Control Subsystem (RACS) as seen in the coming section.

7.2 Quality of Service in Next Generation Networks

One of the premises lying behind the transformation of the traditional telecommunications networks is Quality of Service (QoS). QoS can be defined on several levels. On the lowest level, QoS can be defined using a set of technical parameters related to, for example, delays and jitter in networks ([22]). It is also possible to use a more high-level perspective and define QoS as the degree to which a network or networks can fulfill user expectations. Today's Internet is a best-effort alternative in the sense that most users are treated as equals. As bandwidth requirements for future services are set to grow, the NGN vision is to improve on the best-effort Internet.

There are basically two strategies that can be used to deliver QoS: generous dimensioning or QoS control ([D3]). In this context, generous dimensioning means providing enough network resources to ensure that a suitable number of simultaneous users can utilize the network without unacceptable service degradation. In circuit-switched networks, generous dimensioning has been the prevalent mechanism to ensure QoS. As packet transport becomes more and more wide-spread, the challenges of using generous dimensioning increase. From a resilience perspective, it is also vital exactly how the suitable number of users is determined since the demands on communications resources during disasters, terrorist attacks or other catastrophic events are very different from the situations that operators use to dimension their networks on a commercial basis. QoS control on the other hand is based on the ability to continuously monitor the available network resources combined with connection admission control so that only those services where the network can guarantee a suitable bandwidth are accepted.

The strategies described here, QoS control and generous provisioning, are not mutually exclusive. An operator could use generous provisioning in the core network and deploy QoS control functions in access networks. It is also important to view QoS in a more general context where several networks are used to deliver a service. In this case, QoS signaling parameters have to be exchanged between the networks to provide as much seamlessness as possible even though the networks can be heterogeneous and the underlying technical mechanisms used to deliver QoS in the respective networks can be very different. Questions like these are actively being pursued in international standards organizations.

The development of QoS control mechanisms are shared between a number of standardisation bodies and forums ([D6]). In the ETSI NGN architecture, RACS is the NGN subsystem responsible for elements of policy control, resource reservation and admission control ([4]). The main function of the RACS system is to provide policy based transport control services to applications, so that these applications can request for and reserve transport resources. For Release 1, RACS is limited to provide policy based transport control services within the access networks and at points of interconnection between core networks. There is no requirement for RACS to provide service coverage for core networks themselves or to customer networks. RACS is supposed to be able to simultaneously support up to eight different priority types, where the number of priorities can be a national requirement.

7.3 Other Resilience Aspects of Next Generation Networks

Resilience in a telecommunication network can be defined as a networks ability to quickly recover from or easily adjust to changes due to damage, reduced capacity, congestion, security breaches or faults. Since the primary IEPS objective is to reduce the effects of congestion, failures and faults to enable international calls, resilience aspects of NGNs are important factors to consider in this regard. Priority services should in this regard be seen as one building block increasing NGN resilience for a selected user group.

There is several obvious resilience issues related to QoS control. To make the network bandwidth aware on a higher level, network load has to be measured and controlled in a multitude of network elements. Consider a situation where a finely tuned network is running at a high but manageable level. If a sudden event occurs that somehow changes network topology or available network resources, a QoS control system first has to gather new information regarding the network topology and corresponding utilization levels. From this new information, control mechanisms must be applied to shape or reroute traffic.

One other resilience aspect is overload control to protect NGN's processing resources against surges in demand. With the multitude of protocols that are being used in the NGN setting, a standardised, generic (common to all protocols) overload control mechanisms is being considered within ETSI ([D4]). There is also an ongoing ETSI effort to define requirements for network resilience in emergency communications ([24]).

7.4 Priority Services in Next Generation Networks

The development of priority services takes place in international standardization bodies, where the ITU, IETF and ETSI are the most relevant from our perspective. This development is to a large extent driven by the U.S. need to extend the existing GETS and WPS services to a packet-based environment as seen by a comparison of [D5] and [23]. In the following sections, aspects of priority services in next generation networks are described. Between the standardization bodies, the nomenclature that is used to describe priority services has not been harmonized. Within the ITU, there is an emphasis on telecommunications for disaster relief and later on emergency telecommunications which is somewhat different from the common ETSI or IETF terms. These differences in terminology do not affect the technical work to a noticeable extent, and the distinctions are therefore not elaborated on in this report.

7.4.1 Requirements for Priority Services in NGN Networks

The functional requirements that have been brought forward in the ITU ([23]) contain a number of features coupled to a broader view of priority services than what was presented in section 3.1 as indicated in Table 5 below. The main addition is that general resilience aspects are included.

Table 5 Functional requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks ([23]).

Requirement	Description
Enhanced priority treatment	The technical capabilities sought are similar to those described in earlier sections, for example related to enhanced routing of priority traffic. In connectionless packet-switched networks, it might be necessary to include priority marking for each possible packet which is somewhat different from circuit-switched networks. The access technologies that are mentioned include wireless, satellite, cable, DSL and optical fiber. It is noted that the provision of preferential access to services in evolving networks needs further consideration. The use of pre-emption to free bandwidth and resources is considered as an optional rather than a basic requirement.
Secure networks	The primary security requirements are rapid authentication of authorized users for emergency telecommunications and mechanisms to protect networks against spoofing, intrusion and denial of service.
Location confidentiality	Cf. section 5.3.4.
Restorability	Cf. section 7.3.
Network connectivity	It is stated that it is advisable that networks supporting emergency telecommunications be connected to provide a wide reach. It is also noted that interconnection between network operator boundaries and/or across reference points which constitute national and/or regulatory boundaries need to be considered.
Interoperability	Schemes for interworking between packet-switched and circuit-switched environments need to be considered as priority calls can traverse both of these environments. Interoperability also concerns the use of heterogeneous networks and also configuration issues.
Mobility	Mobility requirements concern both user mobility and the use of transportable, re-deployable and fully mobile network facilities.

Ubiquitous coverage	To provide ubiquitous coverage, public telecommunication infrastructure resources over large geographic areas should form the framework for emergency communications.
Survivability	Cf. section 7.3.
Voice transmission	Voice transmission is likely to form the fundamental telecommunications method for emergency recovery.
Scalable bandwidth	Cf. section 7.2
Reliability/availability	Cf. section 7.3.

7.4.2 Protocols

The primary protocol within NGN is the Session Initiation Protocol, SIP. For priority services, a mechanism has been developed to indicate the request for priority to network resources which is conveyed through the signaling network via the Resource Priority Header ([25]). The primary network entities which may become scarce and congested during emergencies include gateway resources, circuit-switched network resources, receiving end system resources and SIP proxy resources. In [25], two SIP header namespaces are defined: “ets” and “wps”. The “wps” namespace has a strong coupling to the Wireless Priority Service described earlier. Together, the namespaces “ets” or “wps” in session requests require, based on policy, priority treatment in processing and allocating resources to call/session requests and bearer controls. H.248 has in the same manner been augmented to contain indicators for both priority calls and IEPS calls (version 3) to give priority in the signaling between Media Gateways and Media Gateway Controllers. Other protocols that require extensions to support priority service include ([D5]) Diameter, Radius and Cops.

7.4.3 Open Issues

There are several open issues related to the development of support for priority services in packet-based networks. One such issue is related to security as described in section 5.3.4 above. Complementing the discussion of terminal based or IN-based features, there is also a need to analyze to what extent priority calls need to authenticated and authorized between networks to improve security. In non-terminal based AA, it is also important to consider what priority treatment is to be given to a priority call before it reaches the AA network elements. For a priority service involving pre-emption, the security implications has to be weighted against the likelihood that a call will encounter congestion before it is authenticated and given priority treatment.

The technical means that can give priority calls preferential access to processors, databases and other non-transport network resources under congestion also requires further study ([D5]). In the same manner, detailed guidelines on the invocation of QoS mechanisms and other technical features deserve further attention as well as the extension of certain key protocols.

Within this context, it should be noted that the introduction of priority services in national networks involves the interworking between several operators’ network including heterogeneous network technologies. The development of such mechanisms and features, for example related to QoS, will take time.

7.5 Consequences for the Establishment of National IEPS Support

The ongoing evolution of telecommunications networks has several implications for national priority services and, as a consequence, for the future establishment of IEPS support. As we have seen, there is an ongoing development of standards and functions related to priority services which long-term is set to affect the national work on priority services. The primary conclusion here is that priority services in packet-based networks still has to be considered as a work in progress that will require both standardization work as well as technical development before nearing completion.

There are examples where the development of new services for the consumer market will benefit priority services. For example, the drive to furnish NGN's with QoS capabilities will most likely be beneficial for the development and long-term evolution of national priority services as well as IEPS support. The primary reason is that a QoS capable NGN will have the ability to give certain calls preferential access to network resources which is one of the four fundamental technical features of priority services stated earlier in this text.

It is advisable that national user requirements for priority services in packet-based networks are identified and compared to the ongoing development since standards based solutions are likely to be the most cost-effective solution. However, it is far from certain that all operators will deploy the same set of NGN subsystems and QoS mechanisms at any given time.

8 Conclusions, Recommendations and Proposed Implementation Plan

This section summarizes the findings in the report and concludes with a set of recommendations for a future development effort aimed at introducing an IEPS capability in Sweden.

8.1 General Conclusions and Recommendations

The general conclusions from earlier sections are summarized in the table below, complementing the general conclusion that an active participation in international standards bodies is one important factor in the long-term development of cost-effective international priority services.

Table 6 Summary of conclusions and recommendations related to the introduction of IEPS support in national networks.

Issue	Conclusions and Recommendations
Handling of transit networks	An analysis of transit networks involved in international calls has to be made before an IEPS service can be put in place. This analysis should result in service level agreements outlining requirements on international carriers describing actions to be taken for IEPS calls. The minimal requirement is that the international carrier shall preserve IEPS signaling to ensure that priority calls can be given preferential treatment in the destination network. One further basic requirement is that IEPS calls shall be exempt from restrictive network management controls
IEPS service introduction and management	The introduction and management of an IEPS service will primarily involve the principal service customers in the two countries. Their

	responsibilities include: • Pre-implementation planning • Service level agreements with involved international carriers • Overseeing IEPS operation and evolution
Comparison of IEPS features and national capabilities: exemption from restrictive network management controls	It is unlikely that a national priority service will include exemption from restrictive network management controls in the shorter term. The inclusion of such a feature in international gateways is a more limited undertaking and should be included as a part of the pre-implementation feasibility analysis. Long-term, IEPS calls receiving exemption to RNMC is affected by the evolution of technical standards.
Comparison of IEPS features and national capabilities: preferential access to network resources	The primary difficulty in the establishment of a national priority service is the lack of appropriate standardization for wireline networks. In wireless GSM networks standards and implementations are in place in existing systems, capable of giving IEPS calls preferential access to network resources. To that end, interworking procedures, in the form of call marking, marking interpretation and processing arrangements, have to be specified and agreed on.
Comparison of IEPS features and national capabilities: routing enhancements	At the moment, it seems unlikely that a national priority service established in current circuit-switched networks will contain routing enhancements for priority calls as compared to normal calls which obvious consequences for the short-term development of IEPS support. In the longer term, routing enhancements for coming packet-switched networks can be a more feasible option depending on the work on international standards.
Comparison of IEPS features and national capabilities: scope	In the short term, a national priority service will not include technical features ensuring priority inside PBX and Centrex environments.
IEPS security features	In the near term, an IEPS service primary security feature is likely going to be based on the authentication and authorization methods provided through terminal and IN-based methods. Enhanced protection of user data has to be considered as an item for further study. It is advisable to include two further mechanisms: • The continuous monitoring of incoming and outgoing IEPS calls at international gateways • The possibility to dynamically change

	the mapping of incoming and outgoing IEPS calls to different priority levels
IEPS user group restrictions	Restricting the number of people within an eMLPP-based wireless priority service that are entitled to invoke IEPS is not straightforward as it is outside the scope of current standards. Partial solutions exist. From a purely technical perspective, it is advisable to give all national priority users access to the IEPS service.
Evolution of packet-based network technologies	There is currently an ongoing development of standards related to several of the technical features in a general priority service in packet-based networks. From a national standpoint it is important that the national solution is harmonized with this development.
Strategies for implementing IEPS support	There are two basic strategies. The first strategy is the addition of IEPS as a new service so that the IEPS priority indicator is generated in the originating network, independently from any other indicator or condition and is included in the very first signaling message of the call set up procedure. The technical features used by IEPS calls and national priority calls could conceivably be different. The other strategy relies on an existing priority service which is extended at international gateway exchanges by a mapping of priority level indications to and from national priority levels required and applied in the terminating networks. In the short term, the extension of an existing priority service is the only viable option. If the two countries national priority services are similar, extension is likely to be the best alternative. In the longer term, IEPS service addition can be preferable but requires vendor support that is not in place at the moment.

8.2 Outline of IEPS Implementation Plan

The implementation plan proposed in the table below divides the implementation of IEPS into three phases:

- Pre-implementation planning
- Implementation
- Operation and evolution

Table 7 Proposed implementation plan.

Pre-implementation planning	
1	Identification of a national need for an IEPS service
2	Technical and administrative planning including: • Investigation of technical features of the two national priority services

	• Investigation of international carrier networks affecting calls between two countries involving priority features and resilience • Comparison of national user group selection criteria
3	Development of statement of requirements for national operators and international carriers.
4	Definition of criteria for deciding which users should get access to the IEPS service
5	Development of processes describing the interaction between all actors involved in the use, operation and monitoring of an IEPS service
Implementation	
6	Service level agreements between the principal service customers and the involved operators involving technical features and costs
7	Technical implementation of specified capabilities in national operators' and international carriers' networks
8	Testing of the implemented capabilities
Operation and evolution	
9	Continuous evaluation of the operational use and problems associated with the IEPS service
10	Continuous testing of the IEPS service
11	Dialogue around technical, operational or administrative changes affecting IEPS operation
12	Initiation of studies for the long-term evolution of the service based on user requirements developed through dialogues with the user community
13	Active participation in international standards bodies to harmonize national requirements with the international development of future services

9 References

9.1 Documents

[D1] Minutes of the 7 July Review Committee meeting, 2 November 2005, available at http://www.london.gov.uk/assembly/resilience/index.jsp.

[D2] Next Generation Networks: Further consultation, OFCOM, 30 June 2005, available at http://www.ofcom.org.uk/consult/condocs/nxgnfc/.

[D3] Johnson, D. M., QoS control versus generous dimensioning, BT Technology Journal, vol. 23, no 2, 2005.

[D4] Whitehead, M., GOCAP — one standardized overload control for next generation networks, BT Technology Journal, vol. 23, no 1, 2005.

[D5] SAIC, NCS End-to-End Architecture for Next Generation Priority Services, v.1.5: Voice over IP, December, 2005.

[D6] Gallon, C., and Schelén, O., Bandwidth Management in Next Generation Packet Networks, MSF Technical Report, MSF-TR-ARCH-005-FINAL, August, 2005.

[D7] Electronic Communications Act (Lag (2003:389) om elektronisk kommunikation)

[D8] Security Protection Act (Säkerhetsskyddslag, 1996:627).

9.2 Standards and Standards Related Documents

[1]	ITU-T Rec. E.106 (10/2003)	International Emergency Preference Scheme for disaster relief operations
[2]	ETSI EN 300 356-22 (2003-07)	Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP) version 4 for the international interface; Part 22: International Emergency Preference Scheme (IEPS) service
[3]	ETSI DTR 00001 v0.4.9 (2006-02)	Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Release 1 Definition
[4]	ETSI ES 282 003 v1.1.1 (2006-03)	Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-system (RACS); Functional Architecture
[5]	ETSI Workitem 10TD218	Priorities for TISPAN R2
[6]	ITU-T COM 11- R 13 – E	Report 13 from Study Group 11
[7]	ITU-T Q.704 (07/96)	Signalling network functions and messages
[8]	ITU-T M.3350 (05/2004)	TMN service management requirements for information exchange across the TMN X-interface to support provisioning of Emergency Telecommunication Service (ITS)
[9]	ITU-T Q-series, supplement 53 (09/2005)	Signalling requirements to support the International Emergency Preference Scheme (IEPS)
[10]	ITU-T E.350 (03/00)	Dynamic Routing Interworking
[11]	ITU-T E.410 (03/1998)	International network management – General information
[12]	ITU-T E.412 (01/2003)	Network management controls
[13]	ITU-T Q.761 Amendment 2 (12/2002)	Support for the International Emergency Preference Scheme
[14]	ITU-T Q.762 Amendment 1 (12/2002)	Support for the International Emergency Preference Scheme
[15]	ITU-T Q.763 Amendment 2 (12/2002)	Support for the International Emergency Preference Scheme
[16]	ITU-T Q.764 Amendment 2 (12/2002)	Support for the International Emergency Preference Scheme
[17]	ITU-T I.255.4	Priority service
[18]	ITU-T Q.735 (03/93)	Clause 3- Multilevel precedence and preemption
[19]	3GPP TS 22.067 V6.1.0 (2003-06)	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; enhanced Multi-Level Precedence and Pre-emption service (eMLPP) - Stage 1 (Release 6)
[20]	3GPP TR 22.952 V6.1.0 (2004-06)	3rd Generation Partnership Project; Technical Specification Group

		Services and System Aspects; Priority service guide; (Release 6)
[21]	3GPP TS 22.011 V7.0.0 (2004-06)	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service accessibility (Release 7)
[22]	ITU-T Y.1541 (2002)	Network Performance Objectives for IP-Based Services
[23]	ITU-T Y.1271 (10/2004)	Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks
[24]	ETSI TR 102 445 V<0.0.1> (2005-12	Requirements for Emergency Communications Network Resiliency
[25]	RFC 4412	Communications Resource Priority for the Session Initiation Protocol (SIP), Request for Comments, February 2006.