ETSI TR 122 908 V19.0.0 (2025-10)

TECHNICAL REPORT

Universal Mobile Telecommunications System (UMTS);
LTE;
Study on Paging Permission with Access Control (PPAC)
(3GPP TR 22.908 version 19.0.0 Release 19)

Reference
RTR/TSGS-0122908vj00

Keywords
LTE,UMTS

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

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

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

Version x.y.z

where:

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

1 Scope

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

- Identify requirements and aspects for Paging Permission with Access Control.
- Perform a Gap Analysis to assess the ability of existing 3GPP specifications to meet the requirements and aspects.

Regarding use-cases, followings should be studied in order to identify issues which are caused by the existing access control mechanism which does not allow UEs applied the access class restriction to establish terminating calls (non-exhaustive list):

- Priority Service.
- Emergency Service.
- Communication between UEs in the same area where access control is performed

This study should focus on providing this service using the CS/PS domain. This study includes the aspect of originating call and terminating call.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

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

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

[2] 3GPP TS 22.011: "Service accessibility".

[3] 3GPP TS 22.067: "enhanced Multi-Level Precedence and Pre-emption (eMLPP); Stage 1".

[4] 3GPP TR 22.950: "Priority Service feasibility study".

[5] 3GPP TR 22.952: "Priority service guide".

[6] 3GPP TS 23.067: "enhanced Multi-Level Precedence and Pre-emption (eMLPP) - Stage 2".

[7] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".

[8] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[9] 3GPP TS 24.067: "enhanced Multi-Level Precedence and Pre-emption (eMLPP) - Stage 3".

[10] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".

[11] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".

[12] 3GPP TS 43.022: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[13] 3GPP TS 22.101: "Service aspects; Service principles".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [x] 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 [x].

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

3.2 Symbols

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

(void)

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [x] 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 [x].

(ffs)

4 Use cases

4.1 Priority service with congestion of terminating side

There is a priority communication service which is applied to an authorised user (e.g. government, emergency responder) using priority mechanisms such as special access class (i.e. access classes 11 to 15) allocation and high priority level allocation of eMLPP.

The service is effective in giving an important direction in disasters (e.g. earthquakes) which direction is to lead to saving life. This direction should be transferred even if terminating side is in congestion caused by traffic used for confirmation of the safety of people in the disaster areas because the authorised users orders some agencies or people in the disaster areas to take an action for saving life. Use-cases are described below. (Note: not exclusive)

- Case1: Disaster risk management office in government calls to emergency responder within disaster areas in order to supply temporary service to the disaster areas.
- Case2: Ambulance attendant who gets to a rescue site in the disaster areas but does not found out a person calling for help because of unexpected destruction calls to him/her in order to make sure where he/she is.

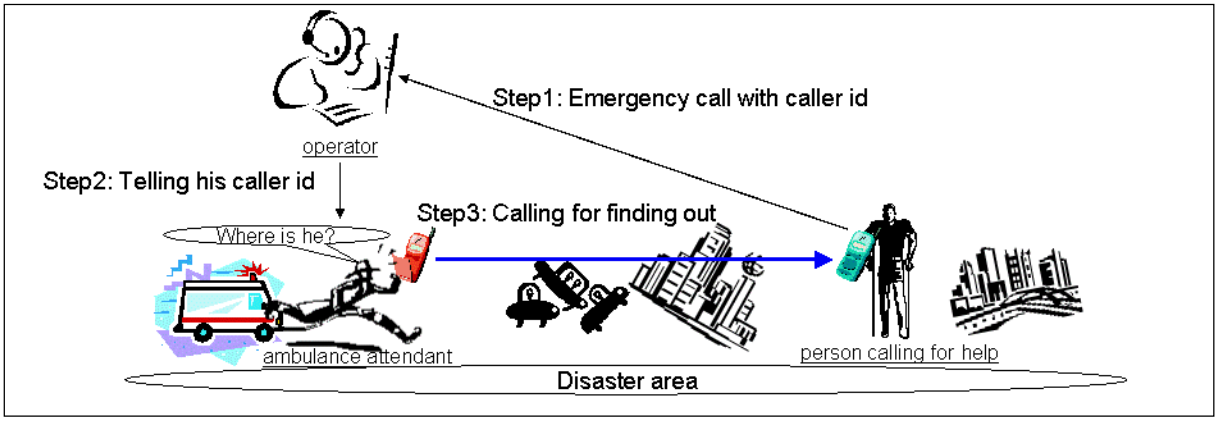


Figure 4.1-1: Case2

- Case3: Firefighter at a fire of high-rise apartment in the disaster areas calls to a person losing his/her way in order to give out directives on the evacuation.

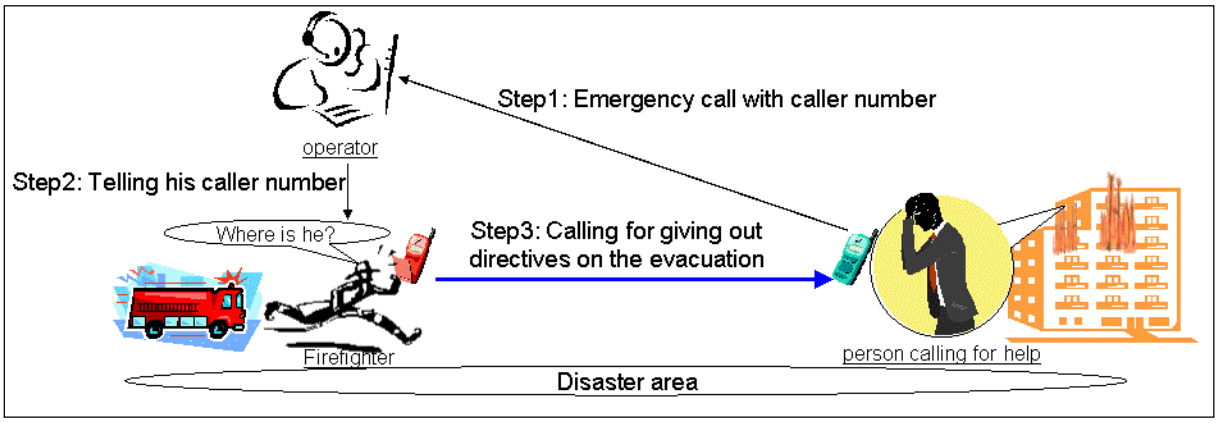


Figure 4.1-2: Case3

Following considerations are identified from subscription aspect. In the case1 both of the originating users and the terminating users are the authorised users. Whereas in the case2 and 3 the originating users are the authorised users and the terminating users are not the authorised users.

4.2 Emergency service call back with congestion of terminating side

A user in the disaster areas sets up an emergency call and it is unfortunately released. At the condition, emergency agencies, e.g. police, would like to call back to the user. The call back should be established even if the network which the user resides in is in congestion caused by traffic used for confirmation of the safety of people in the disaster areas.

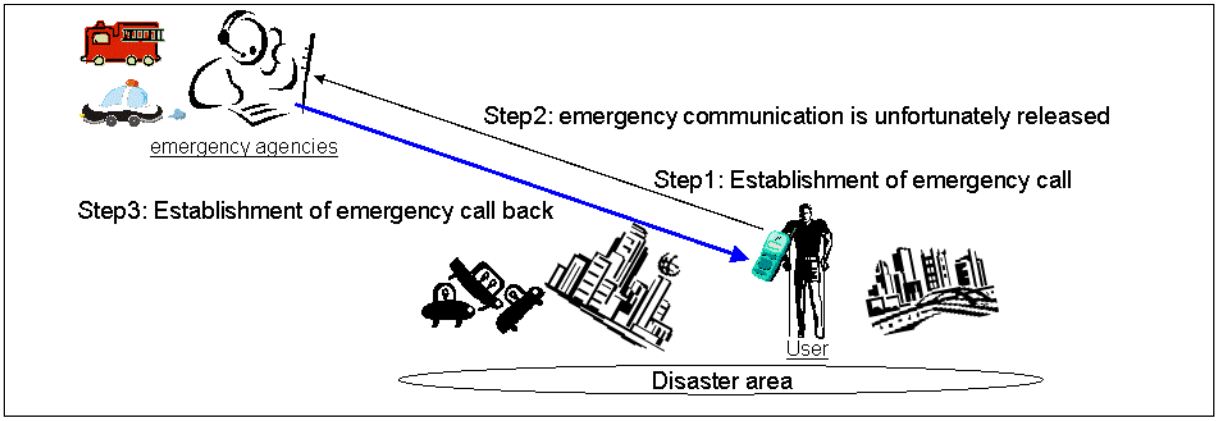


Figure 4.2-1: Use-case of emergency call back

In Japanese background, the emergency call back is important. The new laws in the field of emergency service will go into effect in 1st April 2008. As one of the service requirements in emergency call, once an emergency call is established it can only be released by the PSAP operator and whenever PSAP request to call back, operator is required to successfully establish the call back to the user who made the emergency call.

4.3 Communication between UEs in the same area where access control is performed

There are many earthquakes in Japan and it is hardly possible to predict when and where earthquake happens, therefore the approach to increase installed capacity in all the areas that costs considerable much is impossible. In order to produce communication in congestion conditions in the earthquake, it is not only efficient from installed capacity aspect but also vital from service aspect to perform "access control interval application" that description below explains.

There is an area where access control is performed. In order to allow all the users in the area to setup calls, broadcasting access class numbers are changed at an interval of some seconds. For example, in an interval UEs with access class 0 can perform setup and UEs with access classes 1-9 cannot do setup, in another interval UEs with access class 1 can do setup and UEs with access classes 0, 2-9 cannot do setup.

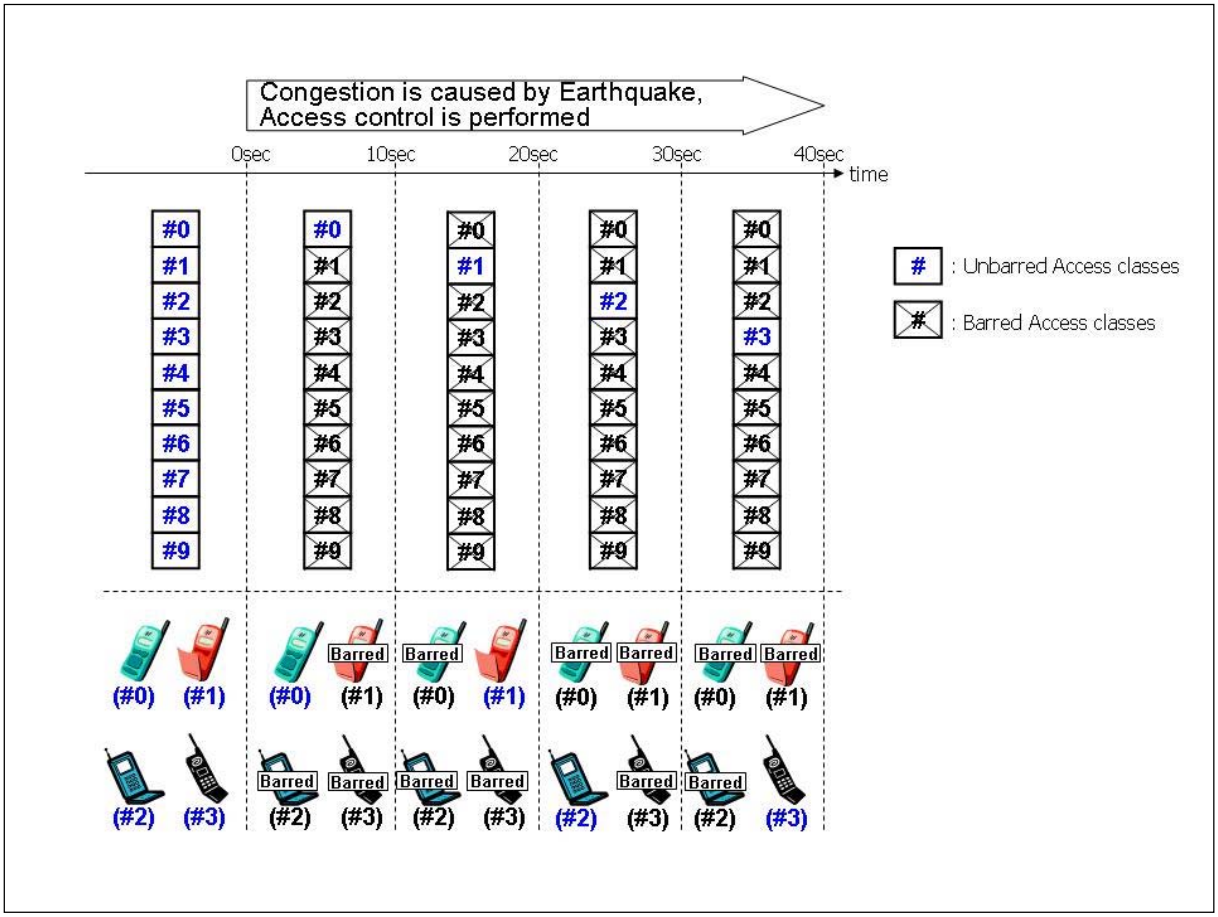
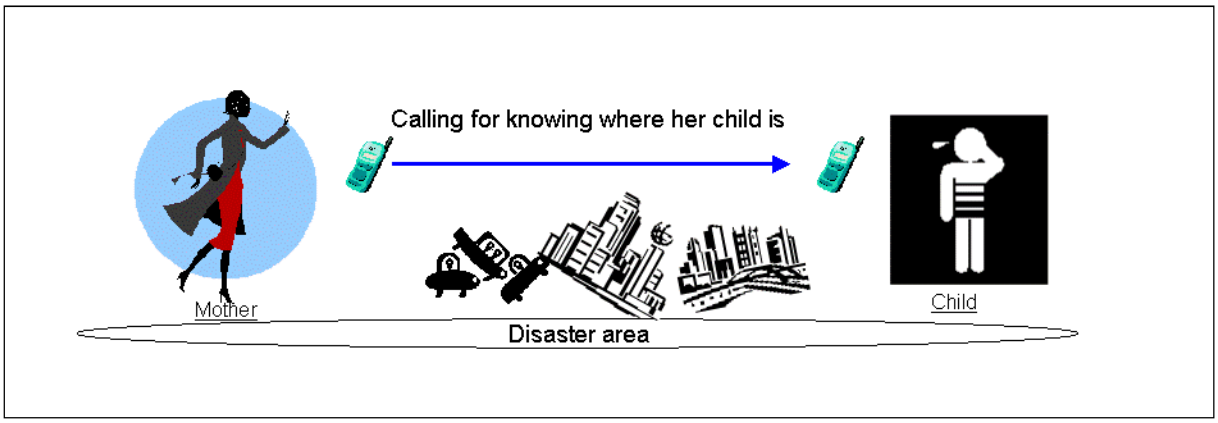


Figure 4.3-1: Access control interval application

Due to access control interval application, the communication between the unauthorised users in the disaster areas is possible. The communication helps users in the emergency situation. Following are use cases.

- A mother calls to her child to know where he/she is in the disaster areas.
- A mother sends a message to her child to know where he/she is in the disaster areas.



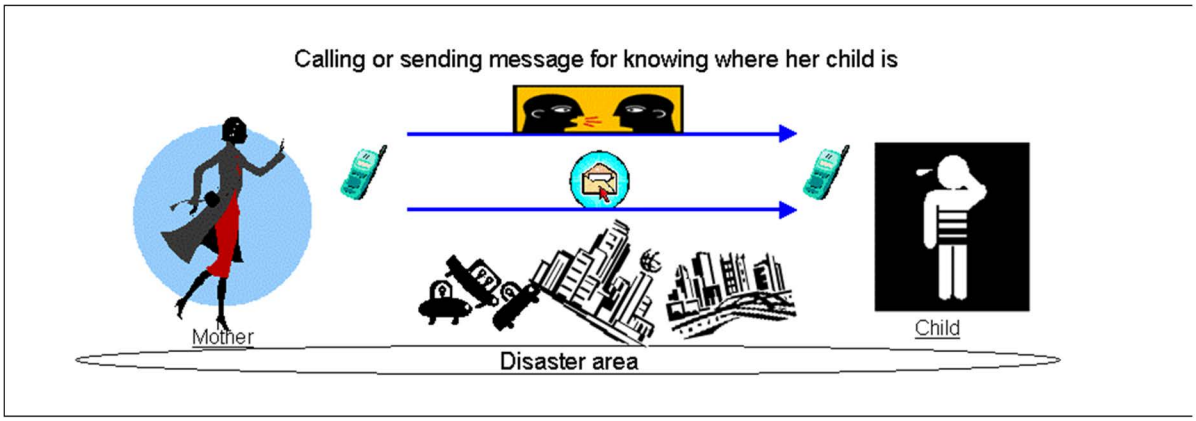


Figure 4.3-2: Use-case of the communication between the unauthorised users

5 Considerations

5.1 Considerations with access class control

Regarding communications in the condition where the originating users are the authorised users and the terminating users in the disasters are not the authorised users as identified in the use cases in section 4.1, there is an issue that the authorised user cannot access to the unauthorised user in the condition that access class control barring is applied to the unauthorised users.

Regarding emergency service call back as identified in section 4.2, there is an issue that emergency service center cannot make callback to the users in the condition that access class control barring is applied to the users.

Regarding the communication using voice or messaging service between the unauthorised users in the area with access control interval application as identified in section 4.3, there is an issue that communication between UE with an access class number and UE with another access class number cannot be established.

Furthermore, it is a further consideration where the current access control mechanism prohibits any access attempts including call control and location registration.

As also described in section 4.3, it is hardly possible to predict when and where a disaster happens. Therefore it is important that a network has to maximize the efficiency of the limited network resources for provisioning of the communications. However, with current access control scheme, even if messages establishing the multimedia telephony calls or messaging service are sent to the UEs that are access class barred, they are not allowed to respond to such messages, consequently resources for the paging messages get wasted. See Figure 5.1-1. Hence, it is a consideration where the multimedia telephony calls and messages to the users to whom access class control barring is applied to end up causing waste of network resources. The resource management efficiency with paging permission under the influence of access class barring is described in Annex X by comparing pattern 3 (i.e. with paging permission) with pattern 2 (i.e. without paging permission).

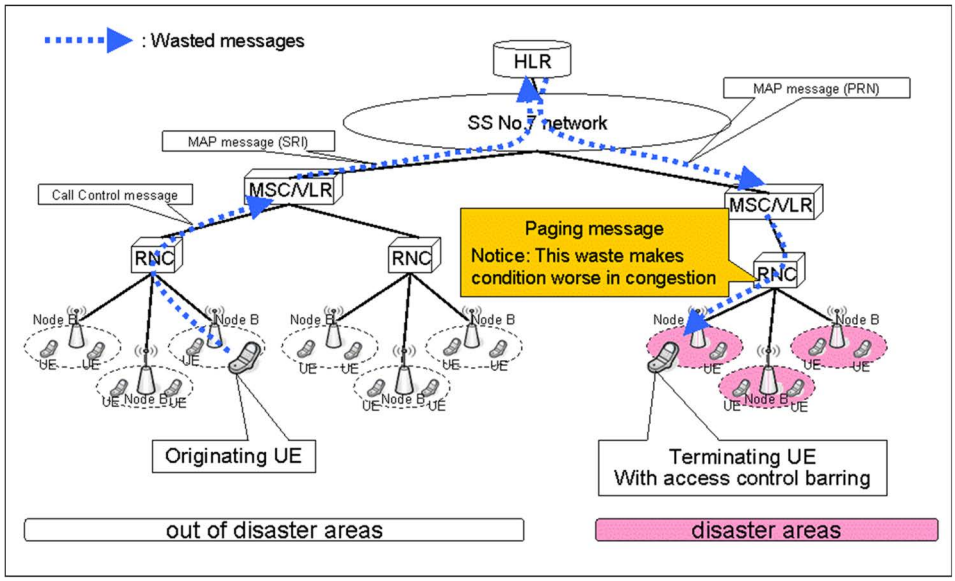


Figure 5.1-1: Waste of resources for the paging messages.

5.2 Considerations with resource reservation of terminating side

Regarding communications in the condition where the originating users are the authorised users and the terminating users in the disasters are not the authorised users as identified in the use cases in section 4.1 and regarding emergency service call back as identified in section 4.2, from the perspective of resource reservation there is an issue that the communications are not surely established because terminating side resource is not guaranteed with current eMLPP and access control.

5.3 Considerations of existing operation and management of access control

Considering existing operation and management of access control, all calls are barred (i.e. both originating and terminating).

6 Gap analysis on current services

6.1 Current functionality

Regarding functionality of access class control, following technical specifications or reports (non-exhaustive) have been investigated.

- 3GPP TS 22.011: "Service accessibility" [2].
- 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3" [8].
- 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode" [10].
- 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification" [11].

  Regarding functionality of have been investigated.

  - 3GPP TS 22.101: "Service aspects; Service principles" [13].

- 3GPP TR 22.950: "Priority Service feasibility study" [4].

- 3GPP TR 22.952: "Priority service guide" [5].
- 3GPP TS 22.067: "enhanced Multi-Level Precedence and Pre-emption (eMLPP); Stage 1" [3].
- 3GPP TS 23.067: "enhanced Multi-Level Precedence and Pre-emption (eMLPP) - Stage 2" [6].
- 3GPP TS 24.067: "enhanced Multi-Level Precedence and Pre-emption (eMLPP) - Stage 3" [9].

6.2 Paging Permission with Access Control gap analysis

The considerations of Paging Permission with Access Control provided in clause 5 which identifies the requirement items. This clause provides a gap-analysis identifying the new capabilities of 3GPP system required for Paging Permission with Access Control in terms of service accessibility and resource allocation and precedence relation.

6.2.1 Service Accessibility

6.2.1.1 Existing capability of Service Accessibility

The capability of Access Control prevents UE from any access attempts (including emergency call attempts) and from responding to pages in specified areas.

Under certain circumstance, the traffic volume exceeds the one that network is capable to handle. Use of access control prevents this overload and provides a mechanism with an aim to maximize the use of communication network resources.

Access restriction information is grouped into two, namely cell access restriction and domain specific access restriction. Followings are the brief introduction of current capability.

Cell access restriction:

If the UE is a member of at least one Access Class which corresponds to the permitted classes as signalled over the air interface, and the Access Class is applicable in the serving network, access attempts are allowed. Otherwise access attempts are not allowed. The Access control with cell access restriction utilizes the Access Classes defined in TS22.101[13] and presented in following table.

Table 6.1: Access Classes

Access Classes	Operation
Class 0-9	Cell access restriction IE for General Use
Class 10	Indication of availability for emergency call from UE with access class 0 to 9
Class 11	Cell access restriction IE for PLMN Use
Class 12	Cell access restriction IE for Security Services
Class 13	Cell access restriction IE for Public Utilities (e.g. water/gas suppliers)
Class 14	Cell access restriction IE for Emergency Services
Class 15	Cell access restriction IE for PLMN Staff

Domain specific access restriction (optional):

Optionally, a network configures with domain specific access control scheme where the network performs access control based on the domain. The detail procedure is defined in TS24.008[8], and the Access control with domain specific restriction utilizes the domain specific access restriction information element defined in TS25.331 and presented in following table.

Table 6.2: Domain Specific Access Control basic information elements

Domain	Operation
CS Domain Specific Access Restriction	Domain Specific Access Restriction Parameters for CS domain
PS Domain Specific Access Restriction	Domain Specific Access Restriction Parameters for PS domain

6.2.1.2 New Capability required for Paging Permission with Access Control

Current Service Accessibility prevents a UE to respond to paging signal while the UE is under the influence of access class control as it is described in clause 5. Sharing the exactly same consequences of this constraint among services provided in this TR (e.g. Priority service, Emergency call, and so on) where call origination does not reach to terminating side, the new capabilities in terms of service accessibility are the followings.

- The UE.should be able to respond to a paging request even when it is under class access barring.
- The UE should also be able to respond to specific paging requests

In addition to above, current Service Accessibility prevents location registration. Without location registration, the network may not be able to send paging request to UE correctly in the following cases

- The mobile reachable timer (network timer for periodic registration) is expired, and the UE is implicitly detached, and UE can not perform the registration procedure because of access control.
- The registration area changes, but UE can not perform the registration procedure because of access control.

To provision the successful terminated call with PPAC capability, it is required for UE to perform location registration when the network indicates UE so.

6.2.2 Queuing and pre-emption

6.2.2.1 Existing capability of queuing and pre-emption

The capability of queuing and pre-emption is supported by two basic schemes, namely eMLPP and Priority Service.

The eMLPP service is provided as a network operator's option to a domain of a network. The domain can be the whole network or a subset of the network. The eMLPP provides Precedence and Pre-emption mechanism for prioritization of resource allocation. The Precedence involves assigning a priority level to a call in combination with fast call set-up. A network operator can allocate set-up classes and resource pre-emption capabilities to each priority level. The seven priority levels are defined in TS 22.067[3] and shown in following table.

Table 6.3: Example on eMLPP Priority level and capability of Pre-emption

Priority level	Set-up time	Pre-emption
A	class 1	yes
B	class 2	yes
0	class 2	yes
1	class 3	yes
2	class 3	no
3	class 3	no
4	class 3	no

The calling subscriber priority levels are used in both the originating and the terminating networks. The highest level (A) is used for network internal use (e.g. emergency calls) and the second highest level (B) is also used for the same manner, but also used for subscription basis depends on regional requirements. The other five priority levels are reserved for subscription, and if commonly acknowledged priority levels are supported by all related network elements and the assigned priority level is presumably transparent from call origination to termination, it may be applied globally.

The default priority level is registered by the service provider or with an appropriate control procedure by the subscriber. While the user may select any priority level up to and including her maximum authorized priority level, the maximum authorized priority level shall be stored on the SIM/USIM and it is the mobile station to check that only an authorized level is used for set-up.

For a network to actually act on precedence resource allocation such as seizing of resources (e.g. wireless channel), the pre-emption makes the resource available for precedence call of higher priority. A network shall have the possibility to pre-empt ongoing calls with lower priority at radio interface or the core network side, or at handover of the precedence call to a congested cell. Pre-emption shall be performed only if a network operator allocates the priority level with pre-emption capability.

The eMLPP shall be invoked automatically by the network at call set-up while the precedence level may be provided by the user on a per call basis.

The Priority Service shares the most of the capability with eMLPP as it is analysed in TR 22.950[4]. The capability of Priority Service is to allow an authorised user to obtain priority access to the next available radio (voice or data traffic) channels during situations when PLMN congestion is blocking call attempts. In addition, Priority Service supports priority call progression and call completion to support an “end-to-end” priority call, see TR 22.950[4].

The capability targets a call origination, a call termination, and a call progression of both non-roaming case and roaming case with applicability of voice and date telecommunication services. The basic mechanisms are specified as follows. Priority Service capability is invoked only when requested originating channel is not available, and in such case, priority call has radio resource queuing and trunk queuing precedence over normal call with numerically assigned priority level where 1 is the highest priority level. It is employed with handover capability and charging capability.

Priority call is authorized based on originating subscription; moreover, it provides manual request of Priority Service by adding service code to origination request.

Optionally, Priority service coexists with eMLPP.

6.2.2.2 New Capability required for Paging Permission with Access Control

The capability of prioritization in resource allocation is already provided with eMLPP and Priority Service. With the new capability described in the aspect of service accessibility, there is no reasonable justification of introducing a new capability (e.g. prioritization of paging request) in terms of resource allocation and precedence relation. Therefore, no new capability shall be provided.

7 Conclusion

From the gap analysis, the only new capability identified is to allow UEs with indications from the network to perform location registration and respond to a paging request even though it is under access class barring conditions to complete certain classes of calls or messages (e.g. calls from emergency personnel, …).

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

Annex A:
Analysis of provisioning of communication between the unauthorised users in the disaster areas

A.1 Introduction

Provisioning of communication between the unauthorised users, with access control interval application, leads to effective and efficient use of network resources. It can be confirmed of the effectiveness and efficiency in the traffic analysis in the 2005 Miyagi Earthquake. There are two types of the effectiveness and efficiency. One is that Congestion with access control interval application ceases earlier than that without them. It is efficient from the perspective of operation and management. The other is that the users can make sure of safety of their families, relatives, and friends. With permitting terminating calls to the users applied access control barring in addition to the access control interval application, the effectiveness and efficiency get better.

A.2 Model for analysis

A.2.1 Model case

Traffic is based on national communication in Japan, so the total number of the users is about 45,000,000. Numbers of UEs applied access class barring are based on population in the Miyagi prefecture, so the number is about 3,000,000.

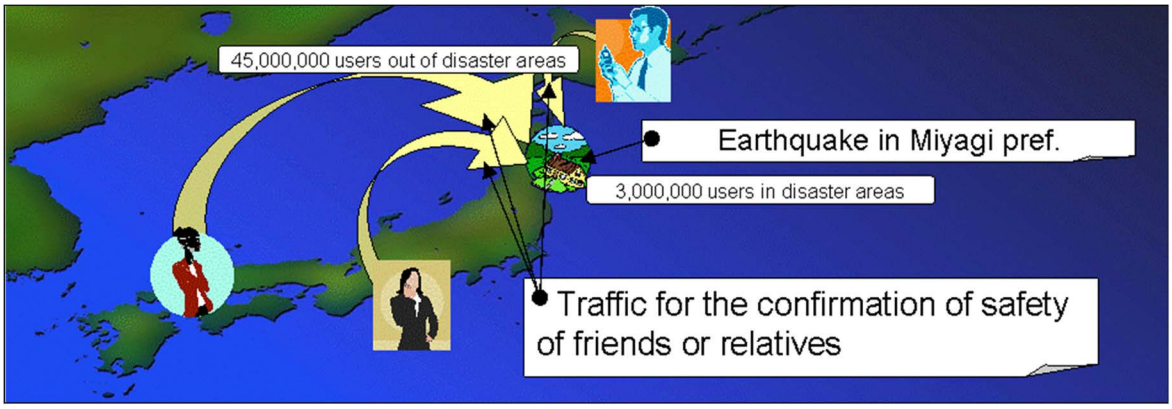


Figure A.2-1: Image of traffic for the safety confirmation

A.2.2 System model

- System architecture

Traffic is calculated, based on the architecture in figure 4.3.1. The architecture for the traffic analysis is comprised of 300 users in disaster areas and 4,200 users out of disaster area, and node b which has 30 channels in the disaster areas.

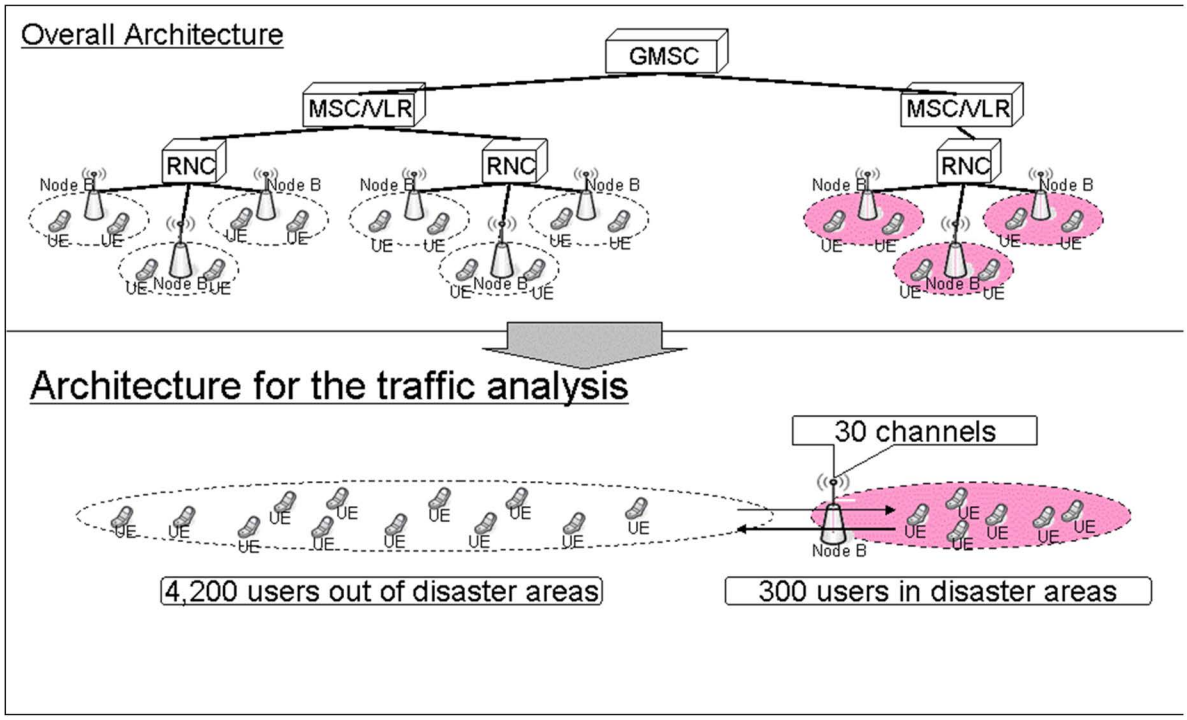


Figure A.2-2: Architecture for the traffic analysis

- Connection model between users

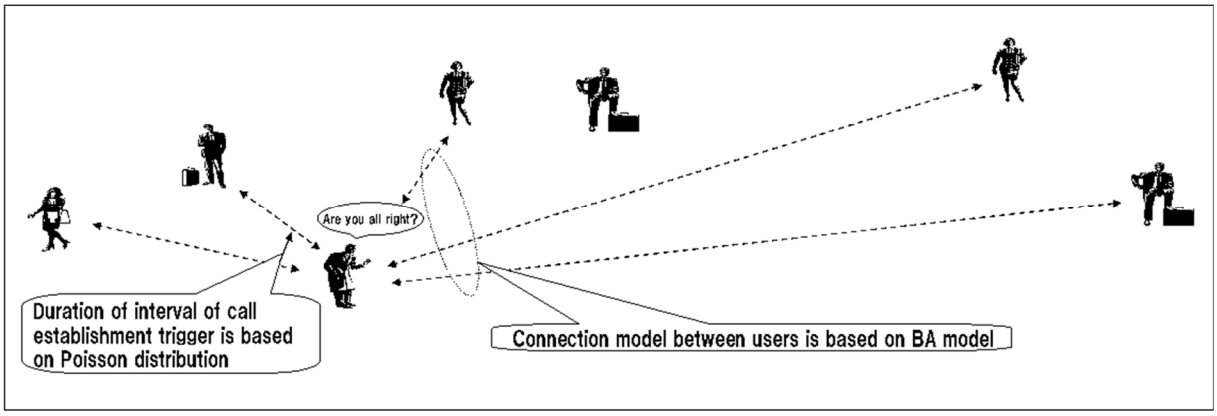


Figure A.2-3 Image of connection model and interval of call establishment trigger

Connection model between users, i.e. who a user calls to among the other users, is based on BA model. The degree distribution of the BA Model follows a power law. The degree distribution resulting from the BA model is scale free. In the model users do not move from disaster areas to non-disaster areas, and vice versa.

Regarding BA model, average number of users for different time length is 3.3, and an initial network of m0 nodes is 2.

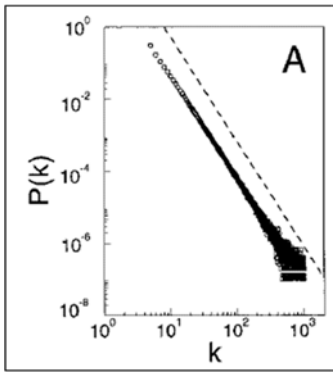


Figure A.2-4: Degree distribution of the BA Model (P(k)~P-3)

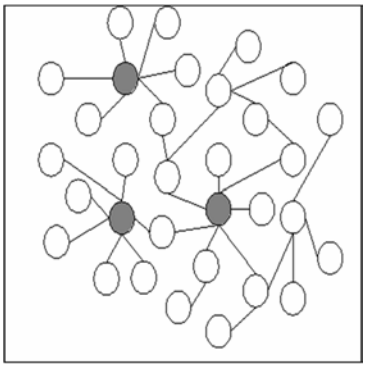


Figure A.2-5: Scale free network

- Interval of call establishment trigger

An originating user continues to trigger establishment of a call to each terminating user until the calls to all the terminating users can be successfully established. If the one of the terminating users trigger establishment and successfully make it, the originating user ceases trying the establishment of a call to the terminating user. Duration of interval of the trigger is based on Poisson distribution. In the traffic analysis the trigger occurs on average every 10 seconds. After the calls to all the terminating users can be successfully established, the average is to be 1,000 seconds (about 17 minutes)

A.2.3 Resource allocation

Channel resource allocation procedure in Node B is based on queuing theory. Duration of holding a channel is based on Poisson distribution. In the traffic analysis average of duration of holding channels is 30 seconds.

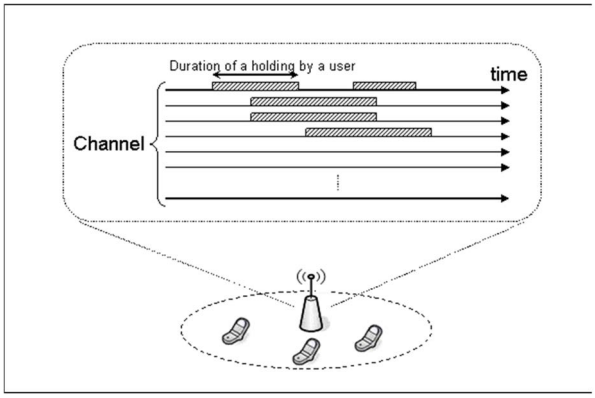


Figure A.2-6: Channel resource allocation

A.2.4 Access Class Barring

UEs of users in the disaster areas are applied access control barring. With the access control interval application, nine out of ten UEs are applied access class restriction. Duration of access control interval is 5 seconds.

A.2.5 Condition of successful connection establishment

Successful connection establishment without terminating permission in being applied access control barring is following procedure. Refer to Figure A.2-7.

If the originating UE is NOT holding an ongoing call, if access class barring is NOT applied to the originating UE, if channel resource for originating user is available, if the terminating UE is NOT holding an ongoing, if access class barring is NOT applied to the terminating UE, if channel resource for the terminating UE is available, the call is successfully established.

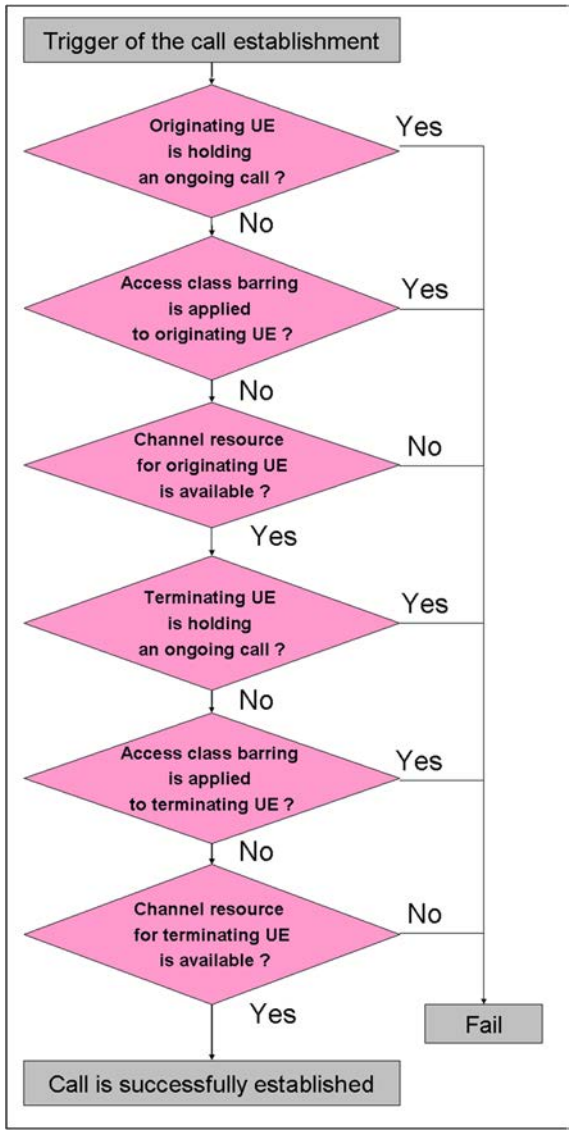


Figure A.2-7: Successful connection establishment procedure without terminating permission

Successful connection establishment with terminating permission in being applied access control barring is following procedure. Refer to Figure A.2-8.

If the originating UE is NOT holding an ongoing call, if access class barring is NOT applied to the originating UE, if channel resource for originating user is available, if the terminating UE is NOT holding an ongoing, if channel resource for the terminating UE is available, the call is successfully established.

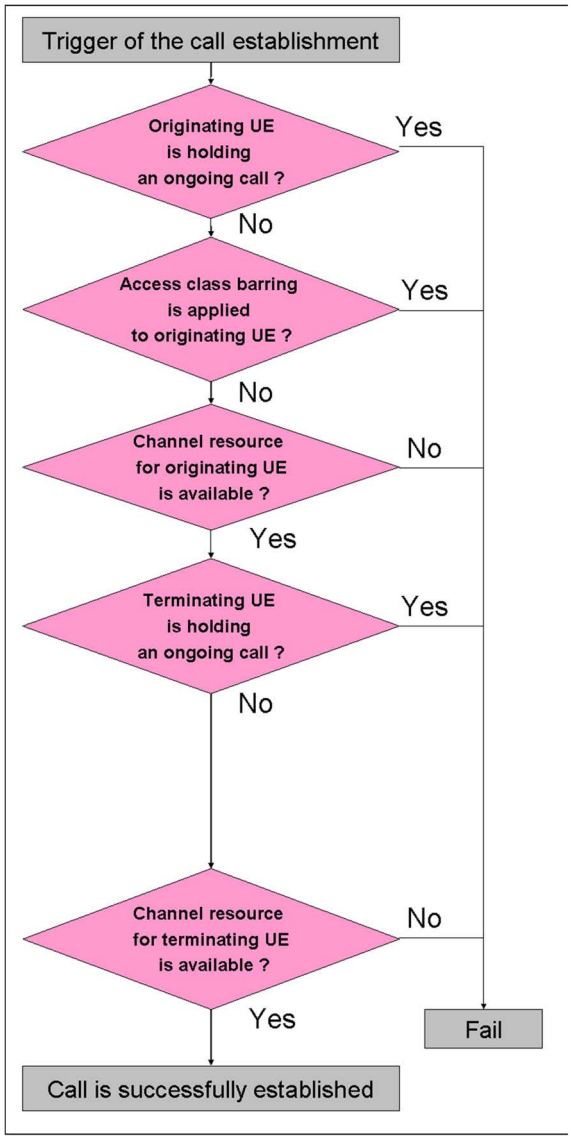


Figure A.2-8: Successful connection establishment procedure with terminating permission

A.3 Analysis

Investing two types of data, the effectiveness and efficiency can be confirmed. One is the channel occupancy within Node B. Channel occupancy means congestion condition. The other is the number of originating users who have not finished the call to all the terminating users. The number is assumed to be number of users who have not confirmed safety of all the relatives and friends.

Data are calculated in three patterns of conditions. Pattern 1 is without access control interval application. Pattern 2 is with access control interval application. Pattern 3 is with access control interval application and with terminating permission with access control barring. Refer to TableA.3-1.

	Without terminating permission with access control barring	With terminating permission with access control barring(Note1)
Without access control interval application	Pattern 1	N/A
With access control interval application	Pattern 2	Pattern 3

TableA.3-1: Three patterns of conditions for data analysis

Note1: In current specification capability of terminating permission with access control barring is impossible.

Considered that 2005 Miyagi earthquake lasted about three hours, duration time of data analysis is 10,000 seconds (about 2hour and 50 minutes) in each pattern. Access class barring with and without interval application is stopped at 5,000 seconds in order to analyse congestion conditions.

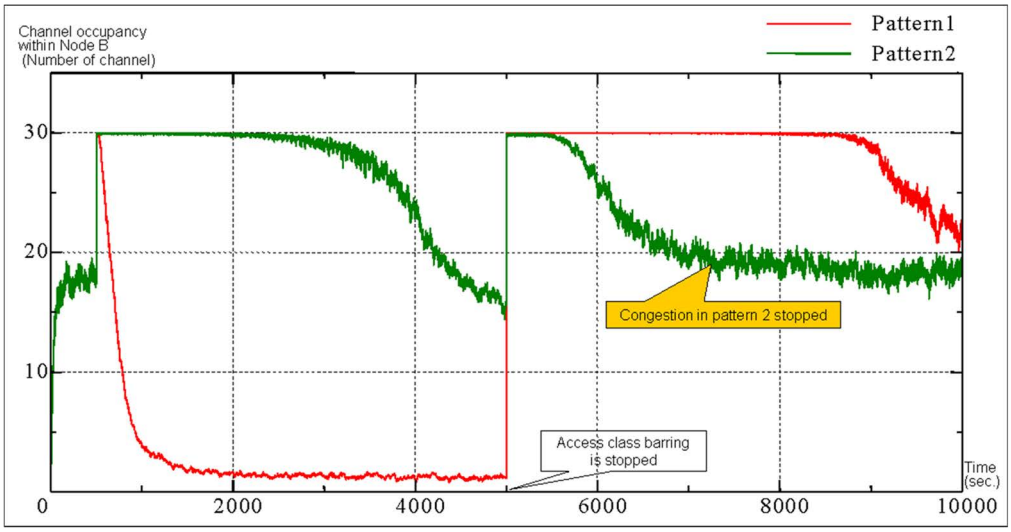


Figure A.3-1: Channel occupancy within Node B in Pattern 1 and 2

Seeing Figure A.3-1, congestion of pattern 2 stopped earlier than that of pattern 1.

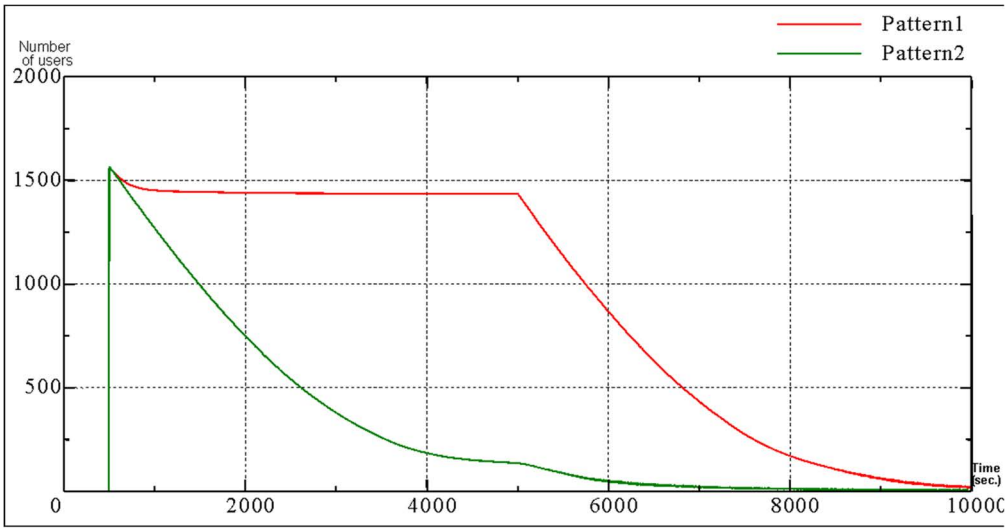


Figure A.3-2: Number of originating users who have not finished the call to all the terminating users in pattern 1 and 2

Seeing Figure A.3-2, users in pattern 2 have finished confirmation of safety of all the relatives and friends earlier than users in pattern 1.

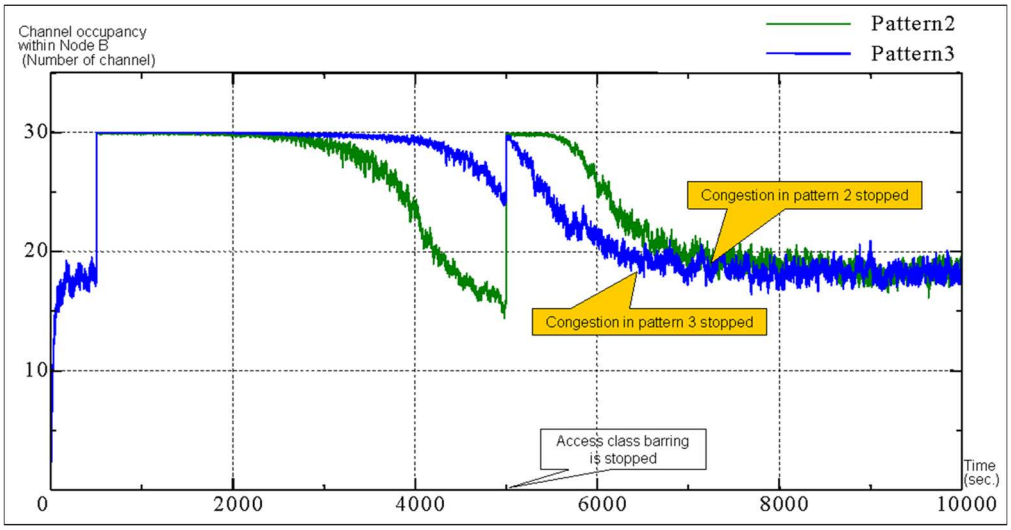


Figure A.3-3: Channel occupancy within Node B of Pattern 2 and 3

Seeing Figure A.3-3, congestion of pattern 3 stopped earlier than that of pattern 2.

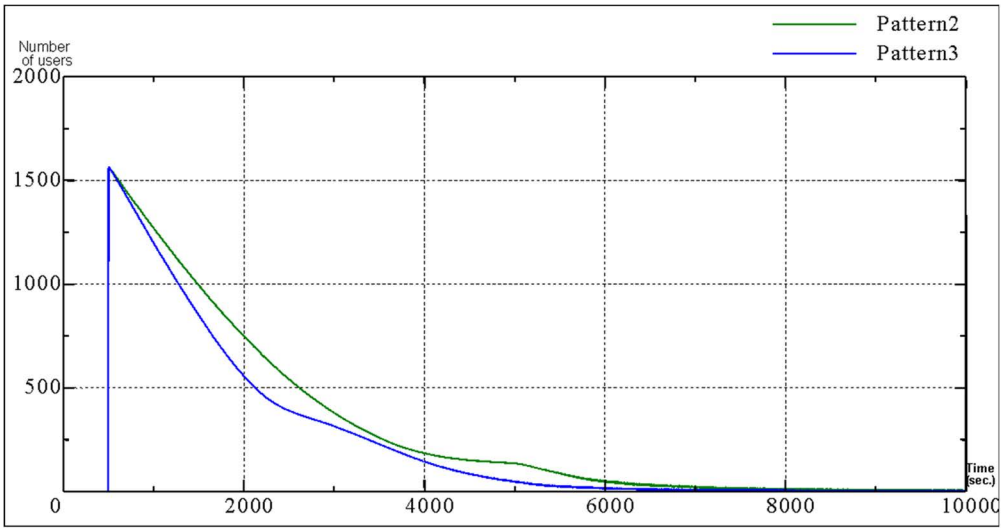


Figure A.3-4: Number of originating users who have not finished the call to all the terminating users in pattern 2 and 3

Seeing Figure A.3-4, users in pattern 3 have finished confirmation of safety of all the relatives and friends earlier than users in pattern 2.

In sum, access control interval application makes both of the effectiveness from the perspective of producing value to the users and efficiency from the perspective of resource management be enhanced, additionally terminating permission with access control barring makes them be enhanced. Therefore provisioning of communication between the unauthorised users in the disaster areas is effective and efficient.

Annex B:
Issues

B.1 Introduction

This clause identifies the issues, which are not within the scope of SA1 WG; thus, this clause is not to restrict further technical work.

B.2 Issue and conclusion

Impact of PPAC function on the UE

The PPAC applies to either all UEs or to a group of UEs

- In the present TR the use-case of an emergency situation is described and this is not a subscription-based service; therefore PPAC capability applies to all UEs or to a group of UEs.
- PPAC is not only for communication from authorized users (e.g. government, emergency responder) to unauthorized users but it includes the case of communication between unauthorized users. If the PPAC capability is different for each use-case, the originating side will be a key player, but differentiating the solution for each use-case is not a appropriate way forward. Therefore, PPAC should be independent from the capabilities of the originating side and PPAC is essentially the capability in terminating side. Thus where the capability is within terminating side, PPAC capability applies to all UEs or to a group of UEs.
- Current access class restriction or domain-specific access control applies to all UEs or to a group of UEs, therefore PPAC capability should also apply to all UEs or to a group of UEs.

Conclusion

Considering above, PPAC applies to all UEs or to a group of UEs.

Annex C:
Change history

Change history											
TSG SA#	**SA Doc.**	**SA1 Doc**	**Spec**	**CR**	**Rev**	**Rel**	**Cat**	**Subject/Comment**	**Old**	**New**	**WI**
SP-38	SP-070953	-	22.908	0001	2	Rel-8	B	Clarification on PPAC requirement	8.0.0	8.1.0	PPAC
SP-46	-	-	-	-	-	-	-	Updated to Rel-9 by MCC	8.1.0	9.0.0	
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	
2014-10								Updated to Rel-12 by MCC	11.0.0	12.0.0	
2015-12	-	-	-	-	-	-	-	Updated to Rel-13 by MCC	12.0.0	13.0.0	
2017-03	-	-	-	-	-	-	-	Updated to Rel-14 by MCC	13.0.0	14.0.0	
2018-06	-	-	-	-	-	-	-	Updated to Rel-15 by MCC	14.0.0	15.0.0	
SA#88e	-	-	-	-	-	-	-	Updated to Rel-16 by MCC	15.0.0	16.0.0	
2022-03	-	-	-	-	-	-	-	Updated to Rel-17 by MCC	16.0.0	17.0.0	
2024-03	-	-	-	-	-	-	-	Updated to Rel-18 by MCC (and issue with v.18.0.0 upload)	17.0.0	18.0.1	
2025-10	-	-	-	-	-	-	-	Updated to Rel-19 by MCC	18.0.1	19.0.0	

History

Document history		
V19.0.0	October 2025	Publication