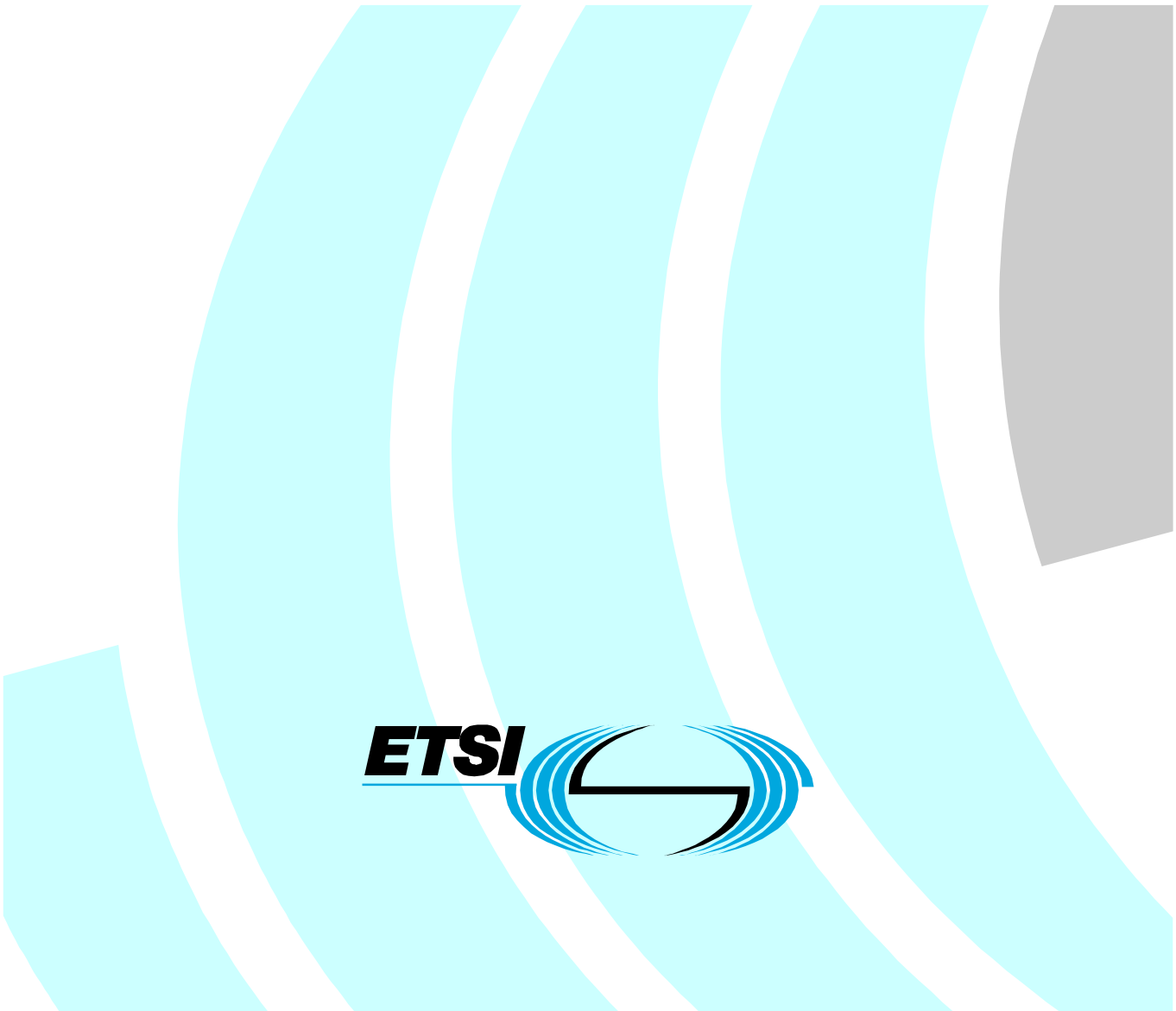
ETSI TS 102 302-2 V5.1.1 (2004-05)

Technical Specification

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 5; Emergency Priority Telecommunications Service (EPTS); Part 2: System description for EPTS in TIPHON networks



Reference
DTS/TISPAN-02010-2-TIPHON_R5

Keywords
emergency, IP, service, telephony, VoIP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

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

The present document is part 2 of a multi-part deliverable covering Emergency Priority Telecommunications Service (EPTS), as identified below:

TR 102 302-1: "Requirements analysis";

TS 102 302-2: "System description for EPTS in TIPHON networks".

1 Scope

The present document defines the operation of the Emergency Priority Telecommunications Service (EPTS) in a generic form. It defines the provision of EPTS, the invocation of EPTS by an authorized user, the validation and authentication mechanisms used to prove the credentials of the EPTS user, the extensions required to the TIPHON generic simple call for EPTS, and the inter-domain carriage of EPTS calls. In addition the mechanisms for revocation of user authorization and of the EPTS service are defined.

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 and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ETSI TR 102 302-1: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Emergency Priority Telecommunications Service (EPTS); Part 1: Requirements analysis".

[2] ETSI TS 101 878 (V4.1.1): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Service Capability Definition; Service Capabilities for TIPHON Release 4".

[3] ETSI TR 101 882: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 5; Protocol Framework Definition and Interface Requirement Definition; General".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

authentication: property by which the correct identity of an entity or party is established with a required assurance

NOTE: The party being authenticated could be a user, subscriber, service provider or network provider.

authorization: act of determining if a particular right, such as access to some resource, can be granted to the presenter of a particular credential

3.2 Abbreviations

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

BICC	Bearer Independent Call Control
CUG	Closed User Group
EPTS	Emergency Priority Telecommunications Service
ETS	Emergency Telecommunications Service
FIFO	First In First Out
ID	IDentifier
ISUP	ISDN User Part
QoS	Quality of Service
SIP	Session Initiation Protocol
SpoA	Service point of Attachment
TRM	Transport Resource Manager

4 Use case examination of EPTS

The use cases shown in figure 1 show the "EPTS_user" and "EPTS_Manager" as specializations of the TISPAN_user, with the addition of the EPTS management use cases. Note that there is a time dependence on the use cases, and the use cases below are described following the time dependence of events.

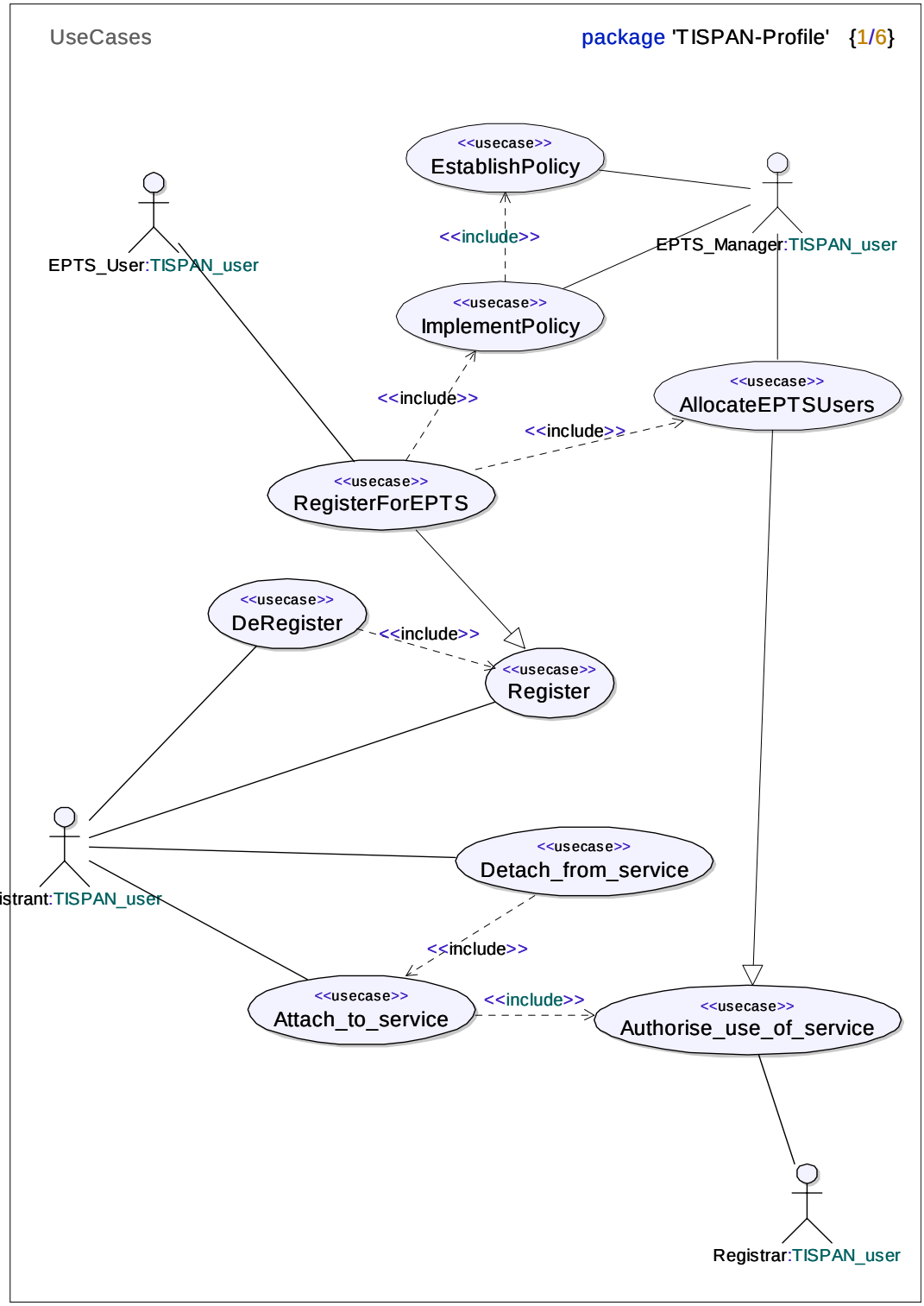


Figure 1: Use case diagram of EPTS service

4.1 Use case 1: Establish policy

The purpose of this use case is to allow the responsible authorities to develop a policy which will be enforced when dealing with circumstances that require the EPTS to be invoked. Policy establishment is a pre-requisite for the use of EPTS. Although the policy establishment is outside the scope of the present document, annex B describes some of the elements that may contribute to policy establishment to develop the EPTS service, and its use.

4.2 Use case 2: Implement policy

The purpose of this use case is to allow the policies defined under use case 1 to be implemented in the system and network to which they apply. This use case is not subject to standardization but is described in annex B.

4.3 Use case 3: Allocate EPTS users

The purpose of this use case is to allow management of the EPTS users. This use case is not subject to standardization but is described in annex B.

An EPTS user, once identified, shall be provisioned in the user-profile by allocation of the EPTS service definitions to the profile. Once provisioned, the user shall be able to attach to the EPTS services.

4.4 Use case 4: Register to EPTS

This use case describes the registration of the EPTS user. It covers the invocation of EPTS service in the profile, allows the user to attach to EPTS SpoA, leading to the usage of EPTS service, subject to EPTS policy. This use case is split into two use cases to describe the role of user and the registrar.

4.4.1 Role of user

Prior to accessing the network resources (for telephony, video, data), the EPTS user shall register with the EPTS service provider. Registration involves:

- identifying and verifying the user, and may include authentication;
- identifying the user location (where applicable).

The user shall provide the user identity registered for the EPTS service, as well as the authentication credentials. Upon successful authentication, the user will receive indication if the registration has been successful or not, and if the user is allowed to use the requested services. The EPTS user may also be informed of duration of the service, which could be a default value defined in policy. If the user receives an authentication failure indication, the user shall re-register by providing the user identity and authentication credentials. If the user receives the "service not available" indication, the user shall abort attempt to register with the registrar. If the user receives a "re-try after" indication, the registrar shall abort the registration request and try to register again after the specified time in the "retry after" indicator.

The EPTS user will receive the identity of the resource manager, SpoA, along with a credential valid for SpoA, from the registrar. The SpoA will provide resources for the user's required services. The user shall use these credentials in its communications requests with the SpoA. The duration of these credentials can be limited to the authentication session.

The EPTS user shall re-register with the registrar, if it wants to continue receiving the required services before the registration expires. If the registration expires, i.e. the authentication session terminates, the user can re-register.

After the successful registration, the user can make use of the network resources, e.g. make telephone calls.

Note that the communications between the registrant and the registrar may be encrypted for added security to maintain the integrity, authenticity and confidentiality of communications.

4.4.2 Role of the Registrar

The registrar is responsible for authenticating and authorizing the EPTS users, and provide or deny them access to network resources.

Upon receipt of the Registration request, the registrar shall check the identity provided by the EPTS user. If the Identity provided corresponds to an existing valid identity held in the profile, the registrar shall proceed to authenticate. If the identity provided does not exist, the registrar shall notify the user that the "authorization failed".

If the authentication credentials are correct, the registrar shall check if the user is allowed to receive the requested services. This authorization may be dictated by the policies such as those described in annex B. If the authentication credentials are incorrect, the registrar shall notify the user that the "authentication failed".

If the user is authorized to receive the requested services, the registrar shall identify a resource manager, SpoA that can provide the EPTS user with the requested services, e.g. telephony. If the EPTS user is authenticated but not authorized to access the requested services, the registrar shall respond with "service not authorized". If the requested service is not available, the registrar shall respond with "Service Not available". If the registrar cannot process the request because of lack of resources, it shall respond with "retry-after" message, indicating a time period after which the registrant can attempt to register again.

The registrar shall then indicate to the SpoA that it has been selected to provide the requested service to the EPTS user, providing it with the identity and credentials of the EPTS user.

The registrar shall respond to the registrant with the "registration successful" indication, along with any public identity that the EPTS user can use.

The registrar shall provide the identity and credentials for the SpoA to the user, indicating that this SpoA will serve the EPTS user for its communications services. The credentials are valid only as long as the authentication session is valid, or per policy arrangement.

4.5 Use case 5: Make EPTS call

After the successful registration, as described in use case 4, the user can make use of the EPTS services allowed in the profile, such as telephony.

This use case is split into two use cases for simplicity, describing the role of user and EPTS service provider (SpoA).

4.5.1 Role of user

The EPTS user shall request the telephony service from the SpoA by providing its identity and credentials. If the user receives "authentication failure" indication, it shall try again with correct user identity and authentication credentials.

If the call can not be set up immediately due to lack of resources, the user may receive an indication that an attempt is being made to set up the call. This could be in the form of a "Call Establishment in progress" indicator.

The user can decide to continue with the call, or abort the call request at any stage during call establishment.

Note that the communications between the EPTS user and the SpoA may be further secured via encryption.

4.5.2 Role of resource manager

When the resource manager, SpoA, receives a request for a call, it checks the user identity and credentials against its records, and upon successful verification, proceeds with call processing. The SpoA identifies the requesting party with a priority level, associated with the user identity, as described in the profile and indicated by registrar during registration. If the SpoA receives a call request from a user whose "authentication session" has expired, the SpoA shall reject the call with an "authentication failed indication". This is because the authentication credentials may only be valid for a predefined time. If the call request contains a user identity that is not registered (attached) with the SpoA, it shall reject the call with "authorization failed" indication.

If the call request contains a valid user ID, but incorrect authentication details, the SpoA shall reject the call with "authentication failed" indicator.

The resource manager shall check the service profile if the calling party is allowed to make call to the called party. If the calling party is not allowed to communicate with the called party (based on CUG information in user profile), the SpoA shall indicate "requested service not available".

If the network is operating in "normal state", then the call may be processed as a normal call [2] and [3].

If the network is experiencing congestion, and the resources are scarce, then the call will be given a preferential treatment, according to the priority level. The preferential treatment requires an alteration to "normal call behaviour". This would allow the call to provide the resources (bandwidth, trunks, ports), that have been reserved for high priority services.

In a state where all high priority resources are not available or in use, instead of declining the call, the SpoA shall try to establish the call with the next set of media descriptor with different QoS requirements. The next media descriptor shall be chosen from the list of media descriptors in the profile. When all the media descriptors have been tried and still the call cannot be established, the call will be held in a queue. As soon as resources are available, the SpoA will allocate that resource to the first call in queue with highest priority. It is important to note that the resources have to available on the end to end basis, i.e. availability of resources at one node, whilst lack of resources at the subsequent node will not lead to the call to be completed. Therefore, the resources shall be reserved end to end.

The resource manger may indicate to EPTS user that the "Call establishment" is in progress. If the EPTS user sends a call clear indication while the call establishment is in progress, the resource manager shall release all reserved resources, and make them available to the next call in queue.

Note that the communications between the resource manager and network nodes may be encrypted.

4.5.3 Making an ETS call (terminating scenario)

In a situation where the called party is busy on another call, the following options can be considered based on the capabilities and policies of the service provider:

- The incoming call may be rejected.
- The incoming call may be held in a queue, and the called party informed of an incoming call. The called party may then either terminate its initial call and accept the incoming call, or put the first call on hold, and accept the second call.
- If the incoming call has a priority higher than existing call, the first call may be held whilst the high priority call is completed to the called party. Note that the low priority call is not terminated.

There are also situations where over ride over supplementary services, such as Incoming call barring, may be required.

5 New service capabilities and modifications to existing service capabilities to support EPTS

This clause identifies the extensions made in TR 101 882 [3] in order to support EPTS.

5.1 Profile group

5.1.1 Additions to data types

5.1.1.1 Service name

"EPTS voice call" has been added as a new "service name".

5.1.1.2 Service credentials

The bearer descriptor has been extended to support "1" to "n" bearer descriptions. This allows subsequent bearers of lower quality to be requested if the initial bearer cannot be provided for the EPTS call.

5.1.2 Modification and extension to service capabilities

5.1.2.1 Add service to profile

Add Service to Profile service capability allows the addition of new services to the profile. Addition of a new service implicitly indicates *authorization* for that service. An EPTS service can be added to the profile by using this service capability. The EPTS service shall remain in the profile as long as the users are authorized to use it. Figure 2 shows the state chart for using this service capability.

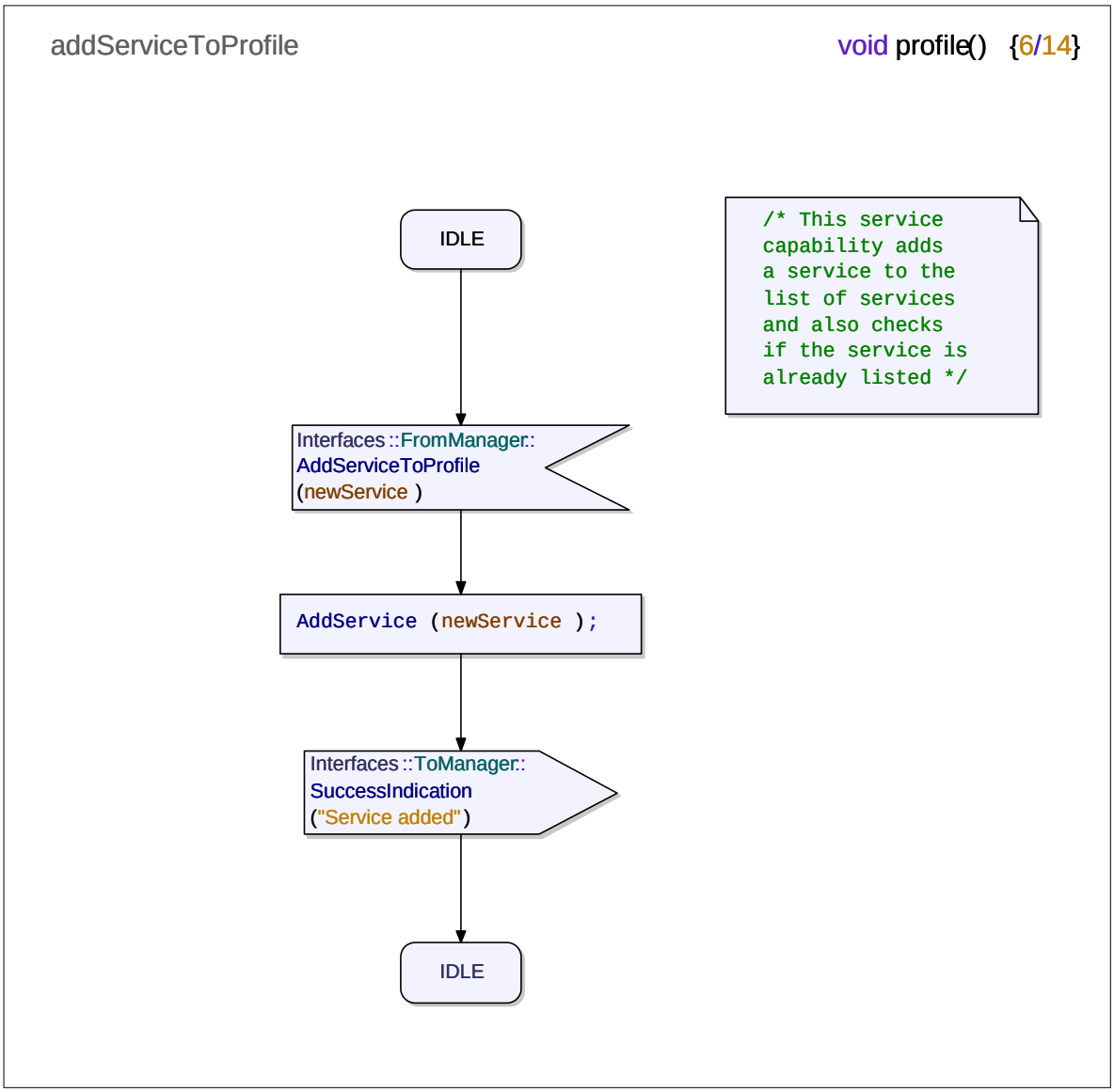


Figure 2: State chart diagram for *add service to profile* service capability

5.1.2.2 Remove service from profile

Remove Service from Profile service capability allows the EPTS service to be removed from the profile. The EPTS service may be removed from the profile, for example, when the emergency no longer exists, or the user is not authorized anymore. Figure 3 shows the state chart diagram to use this service capability.

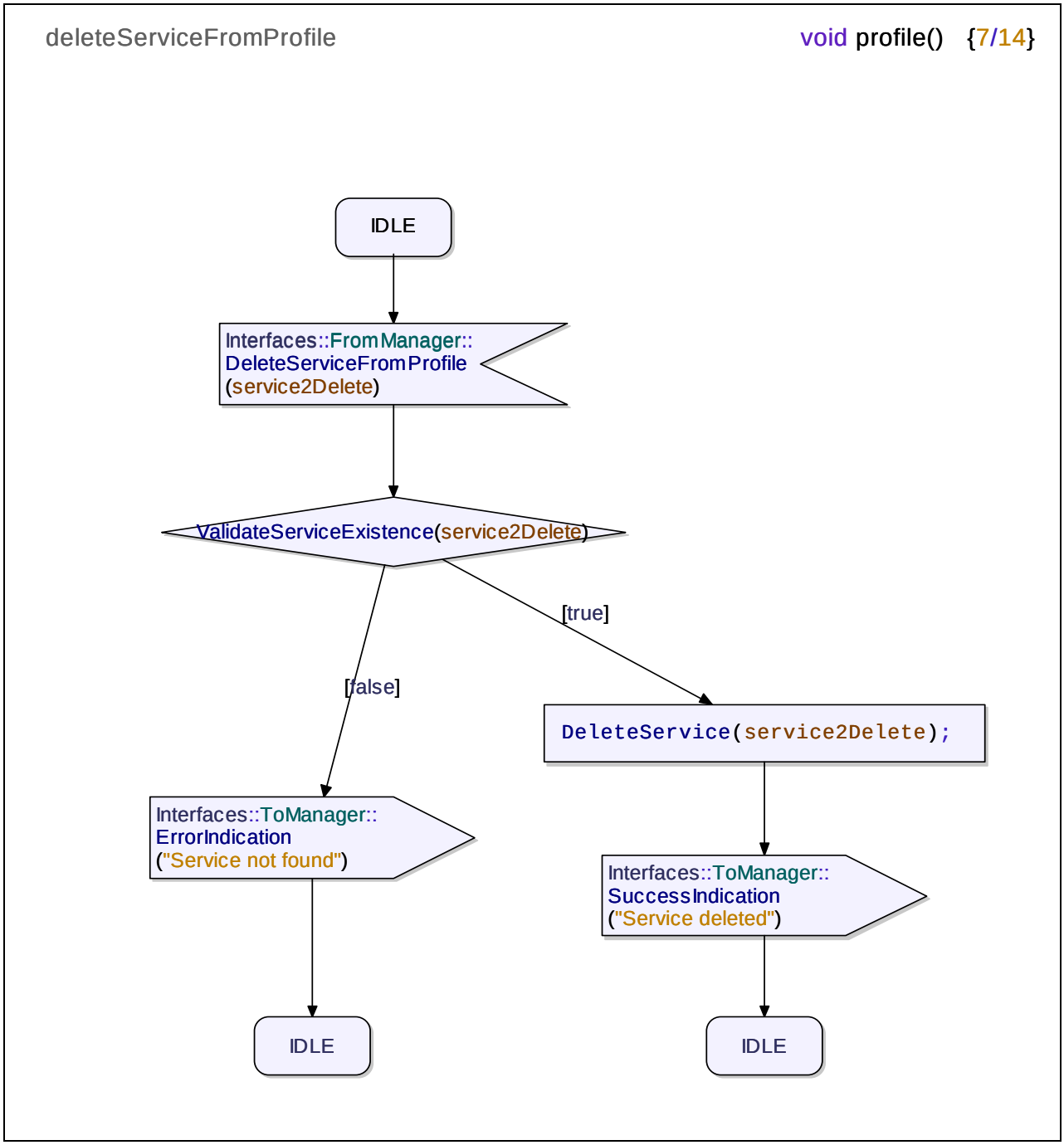


Figure 3: State chart diagram for *delete service from profile* service capability

5.1.2.3 Authentication

The *authenticate* service capability is used to ensure that only the authorized and authenticated users are allowed access to the EPTS service. Within the authenticate service capability, the following capabilities have been added to support a variety of authentication configurations:

- symmetric and asymmetric keying methods;
- single and multi-pass protocols;
- unilateral and mutual authentication. This allows for the profile to authenticate the user, as well as the user to authenticate the EPTS system:
  - bi-directional challenge-response type;
  - able to be initiated either explicitly or as part of the registration procedure;
  - able to be initiated by the terminal or the network;
  - the recipient of the first authentication demand may instigate mutual authentication by use of a mutual authentication indicator, and by sending its challenge together with the response to the first challenge; and
  - where authentication is initiated as part of the registration the authentication timer TA shall always be less than or equal in value to any registration timer.

Considerations have been given to the key management for confidentiality, integrity and authentication. This is described in annex A. The requirements related to the duration of authentication session are also covered in annex A.

TR 101 882 [3] identifies a number of different authentication capabilities. These are illustrated in the figures below and illustrate the following methods of authentication:

- Challenge-Response; and
- Message Authentication Integrity Code.

In addition capabilities are provided to set and clear the authentication method applied to the user profile.

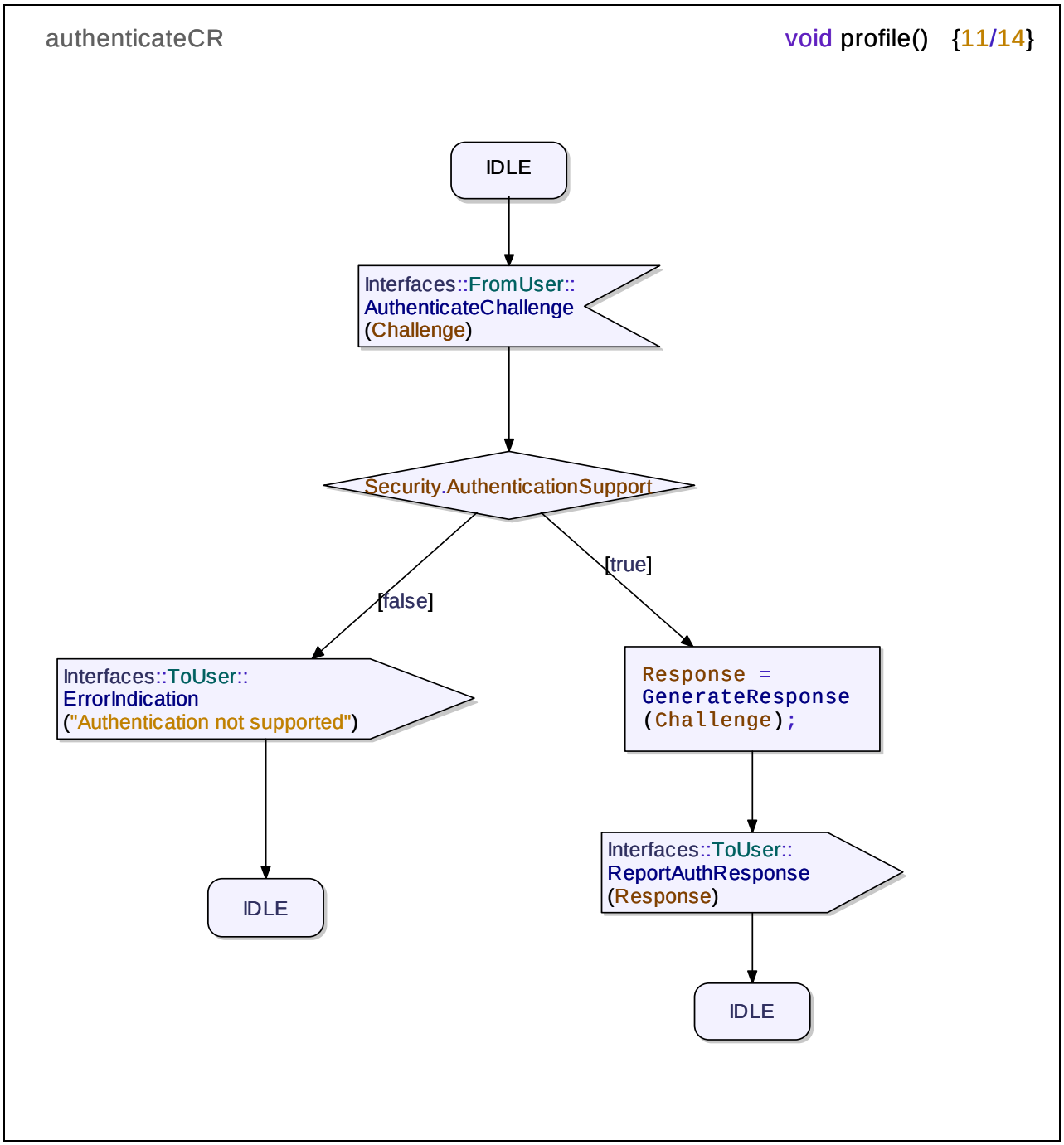


Figure 4: State chart diagram for *Authenticate Challenge Response* service capability

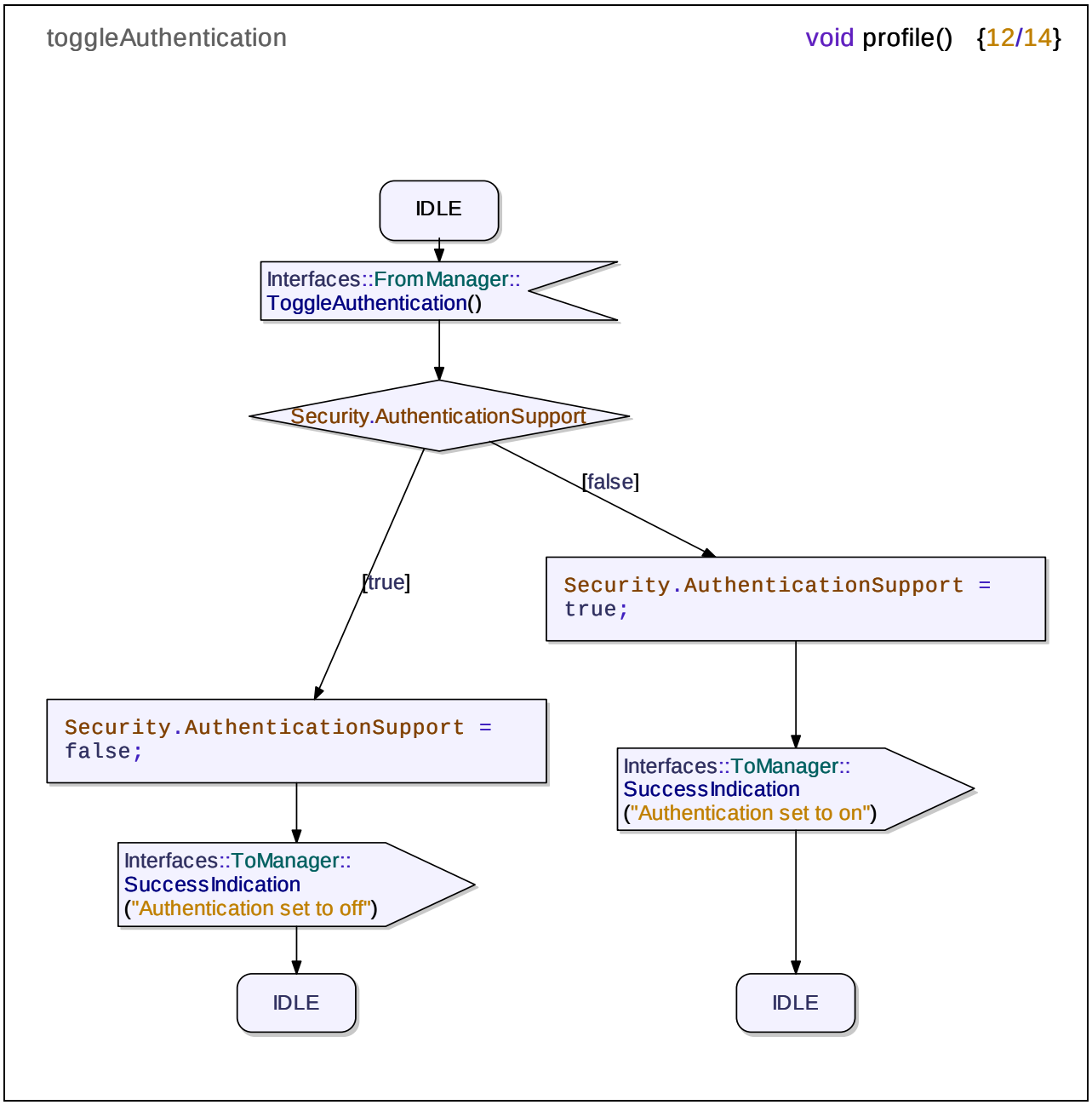


Figure 5: State chart diagram for *Authenticate Toggle* service capability

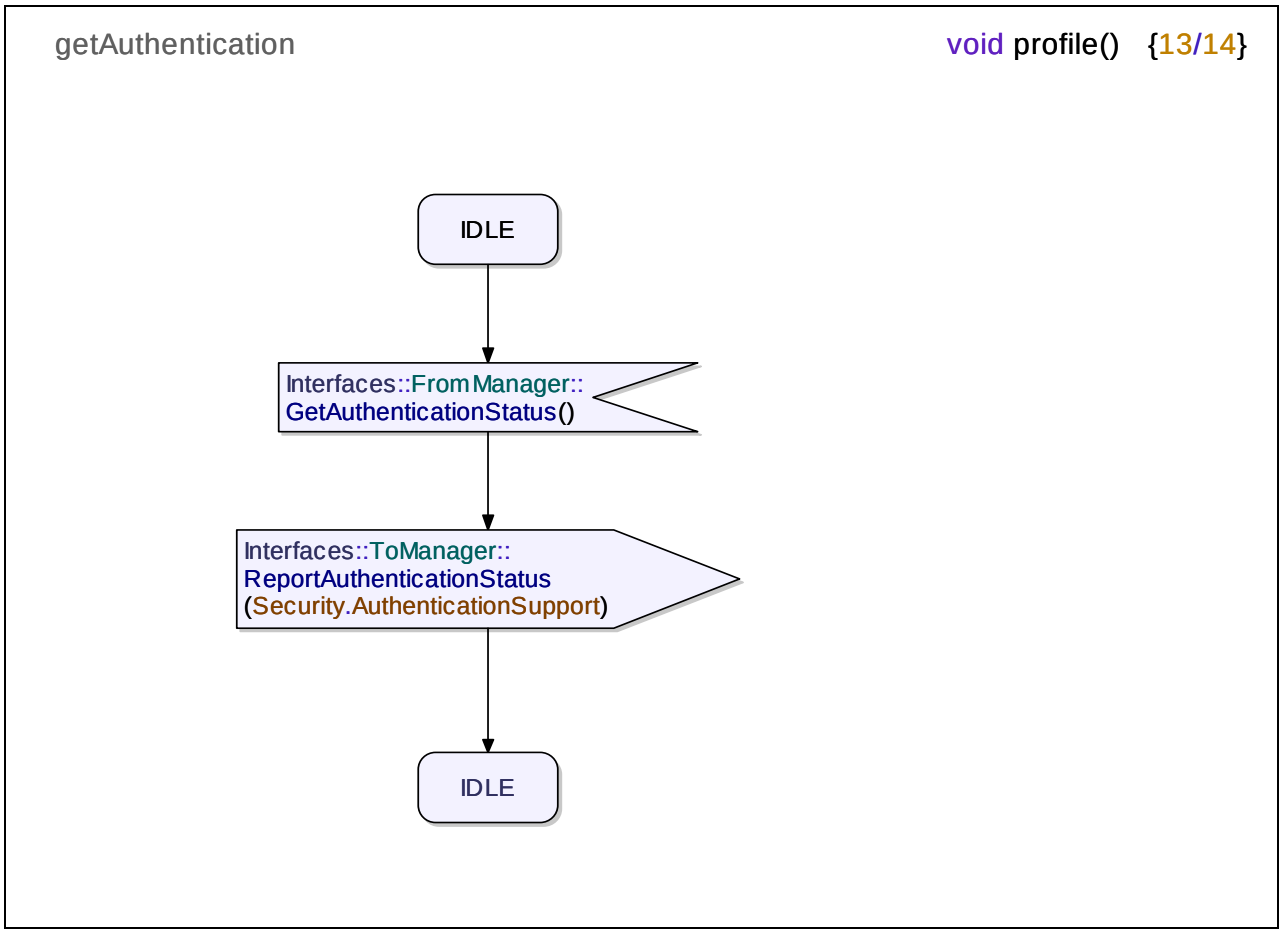


Figure 6: State chart diagram for *Get Authenticate Status* service capability

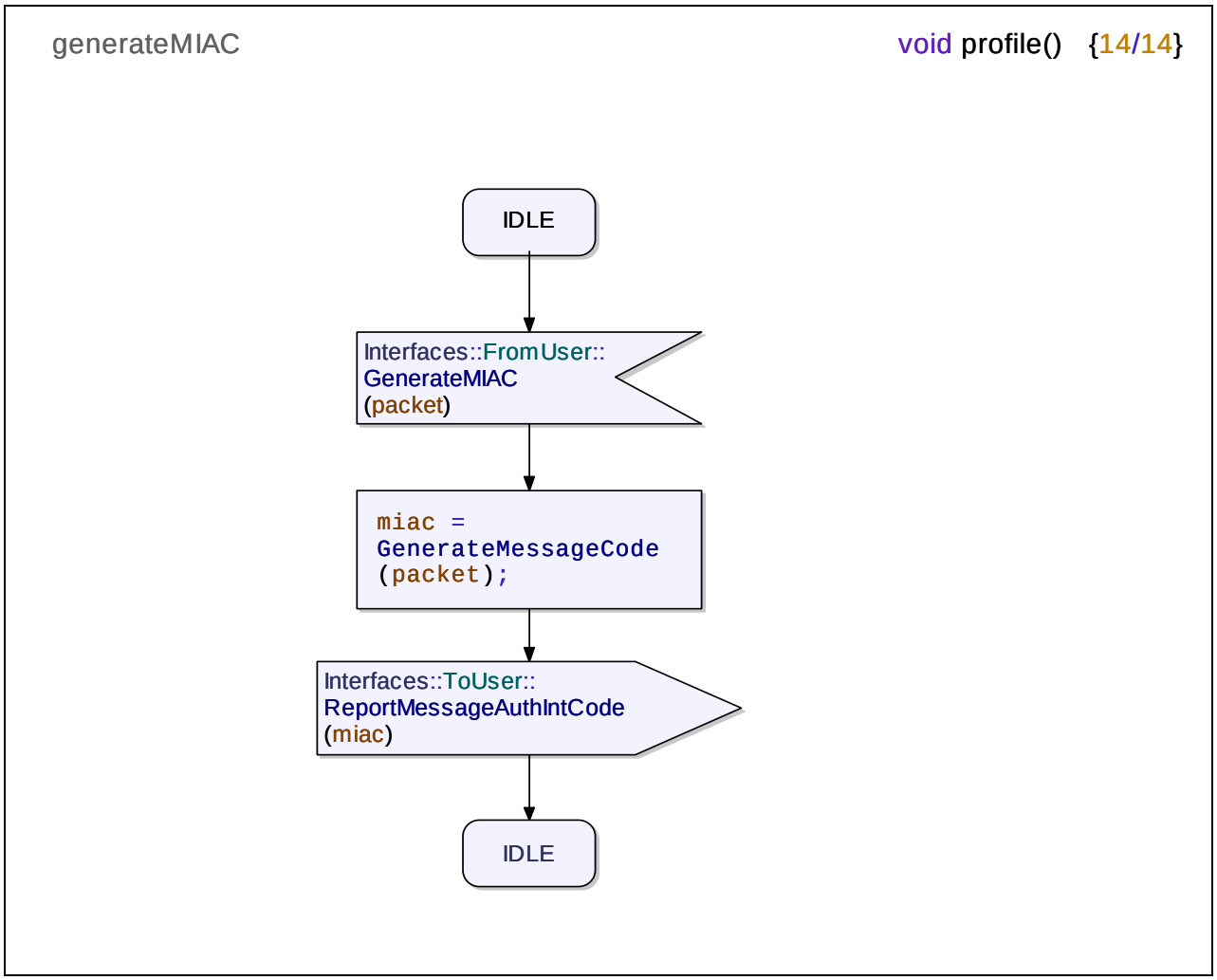


Figure 7: State chart diagram for *Generate Message Integrity and Authentication Code* service capability

5.1.2.4 Interrogate location

This service capability allows the authorized users (authorities) to interrogate location of other authorized users. This may be used to ensure, for example, that only the authorities available in the emergency location are allowed to use the EPTS service. Figure 8 shows the state chart diagram describing the *interrogate location* service capability.

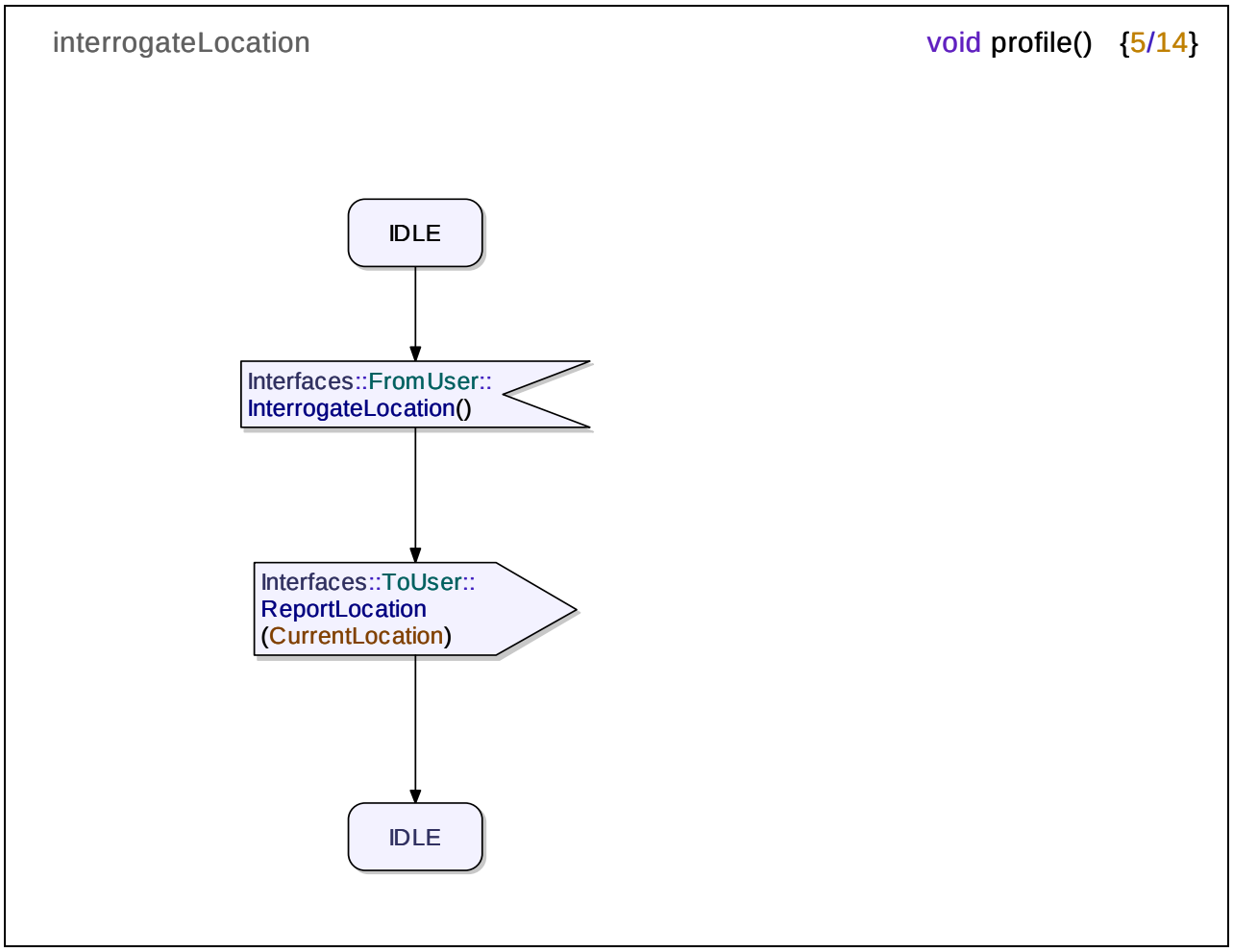


Figure 8: State chart diagram for *interrogate location* service capability

5.2 Call group

When authorized, registered, and attached to an EPTS service, the EPTS user uses the indicated SpoA to obtain the service (where the SpoA may be a telephony platform, an Instant Messaging platform, an e-mail platform or some other network service agent).

The local transport resources available to the SpoA are maintained by a service independent Transport Resource Manager (TRM). The SpoA shall request transport resources from the TRM in accordance with the bearer descriptor element of the service description (see TR 101 882 [3]).

If the network is experiencing congestion, i.e. the transport resources are scarce, the TRM shall give priority to resource requests from the EPTS SpoA.

The general relationship of SpoA to TRM is shown in figure 7 (in which the EPTS-SpoA is shown as a specialization of SpoA, and in which a single TRM acts for many SpoAs).

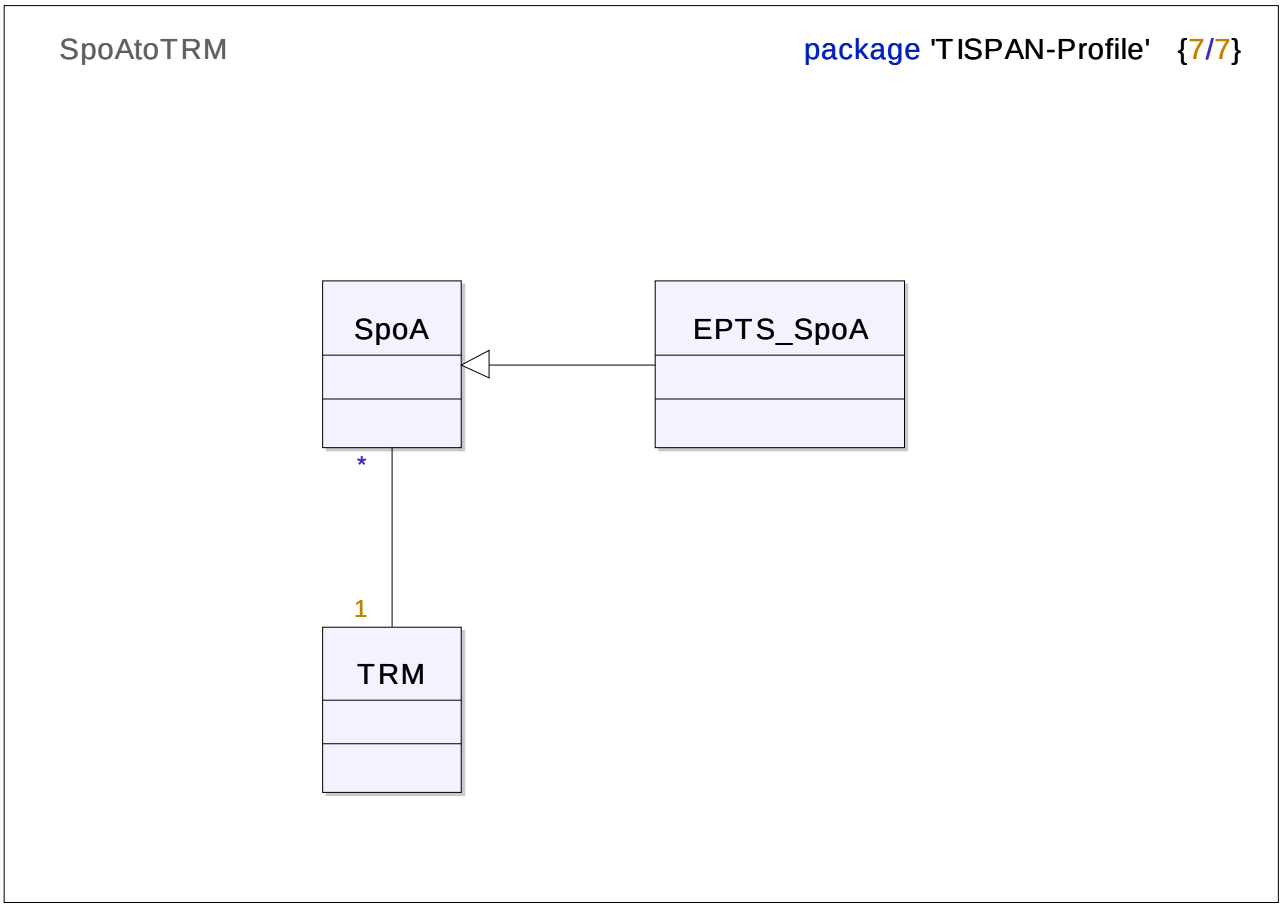


Figure 9: Relationship between SpoA and TRM

5.2.1 Additions to data types

The following data types have been extended to support EPTS service in call service capabilities.

5.2.1.1 Call type

EPTS has been added as a call type allowing the network to recognize the type of call.

5.2.1.2 Call priority

A new class of EPTS has been added to the call priority data type. The EPTS shall have an associated priority level, indicating the priority of the call to applications in the network, leading to the prioritization of call to be completed.

Note that there may be more than one level of priority with which services are provided on a network. The priority level allocated to the EPTS call is subject to network operator policies.

5.2.2 Modification and extension to service capabilities

5.2.2.1 Modify call priority

This service capability allows the priority of the call to be modified in the network. When a user initiates a call, then based on parameters such as EPTS authorization in profile, the ingress node modifies the priority of the call, from normal to EPTS. This leads to preferential treatment in network resource allocation for the call.

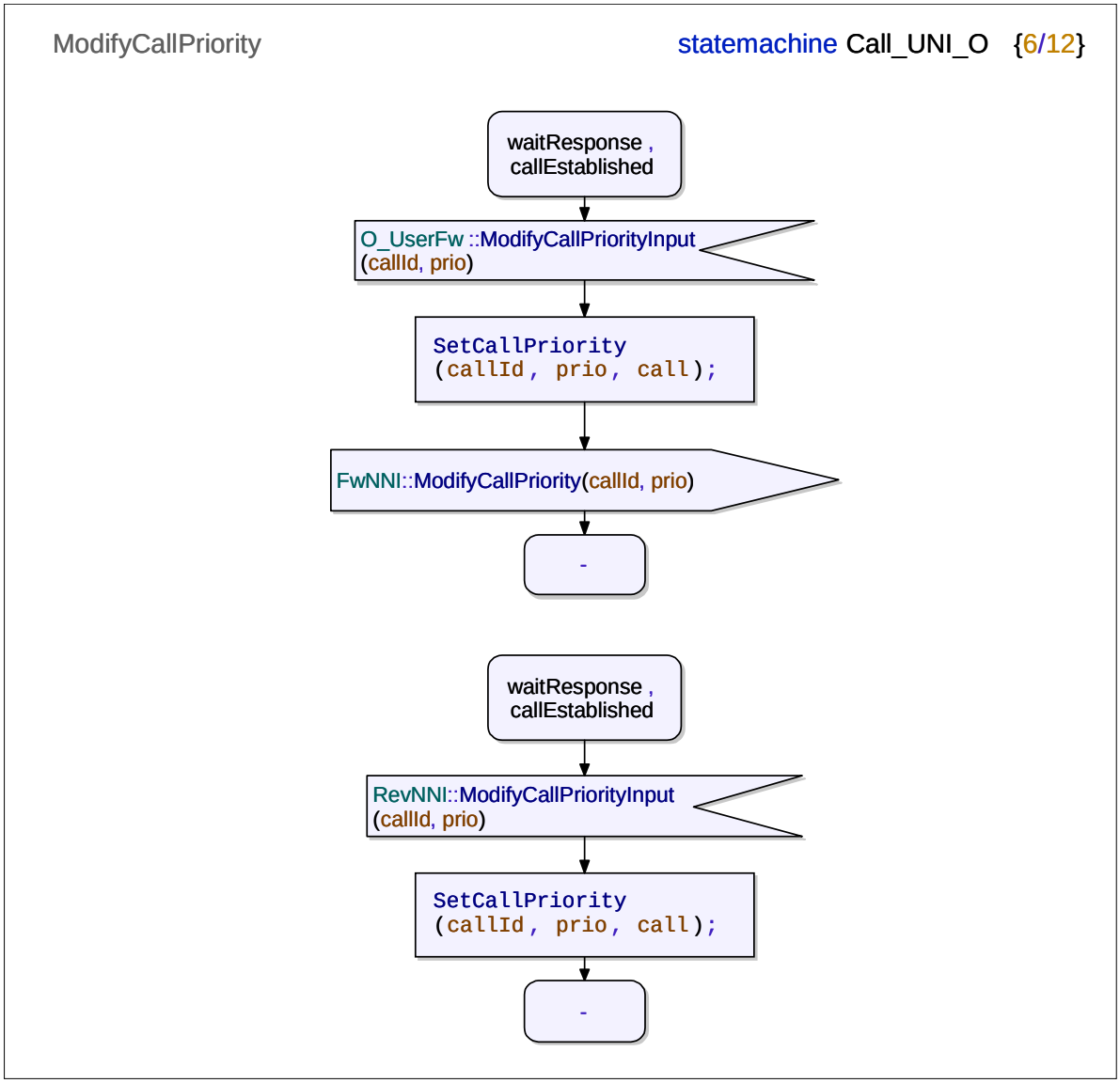


Figure 10: The originating domain *modify call priority* service capability

5.2.2.2 Call set up service capability

The behaviour of the call set up service capability has been changed to accommodate the requirements in TR 102 302-1 [1]. This includes changing the blocking behaviour of telecommunications service to a queuing behaviour. When the requested resource, such as QoS described in bearer descriptor, is not available, the call shall not be rejected, instead the resources for the next supported bearer shall be requested by the call control service capability. There are "1" to "n" bearer descriptors that can be supported by the TIPHON model. When all the bearer descriptors have been tried, and resources are not found, then the call will be queued until resources are made available.

Whilst the call is queued in the network, an indication of "call establishment in progress" may be sent to the user, based on the service provider policies.

5.3 Media group

5.3.1 Addition to data types

The following Media data types have been extended to support the EPTS service.

5.3.1.1 Priority type

EPTS has been added to the media priority type to indicate to the priority of the requested media, to the resource server, such as TRM. This data type is used, for example to indicate to media server that the resources have been requested for the EPTS service, which may allocate the resources reserved for EPTS service.

5.3.2 Extension and modification to media service capabilities

5.3.2.1 Set media encode service capability

The "Set Media Encode" service capability is used to get available media resources. This finds the media resources available that can be used to support the EPTS service. The available media resources are compared with the requested media resources. If the requested media resources are available, then these will be allocated for the EPTS service. If the media resources are not available, or not supported, then an error message "Media not supported" will be returned.

The set media encode service capability can be invoked again by requesting a new media descriptor from the list (as discussed in the call setup service capability).

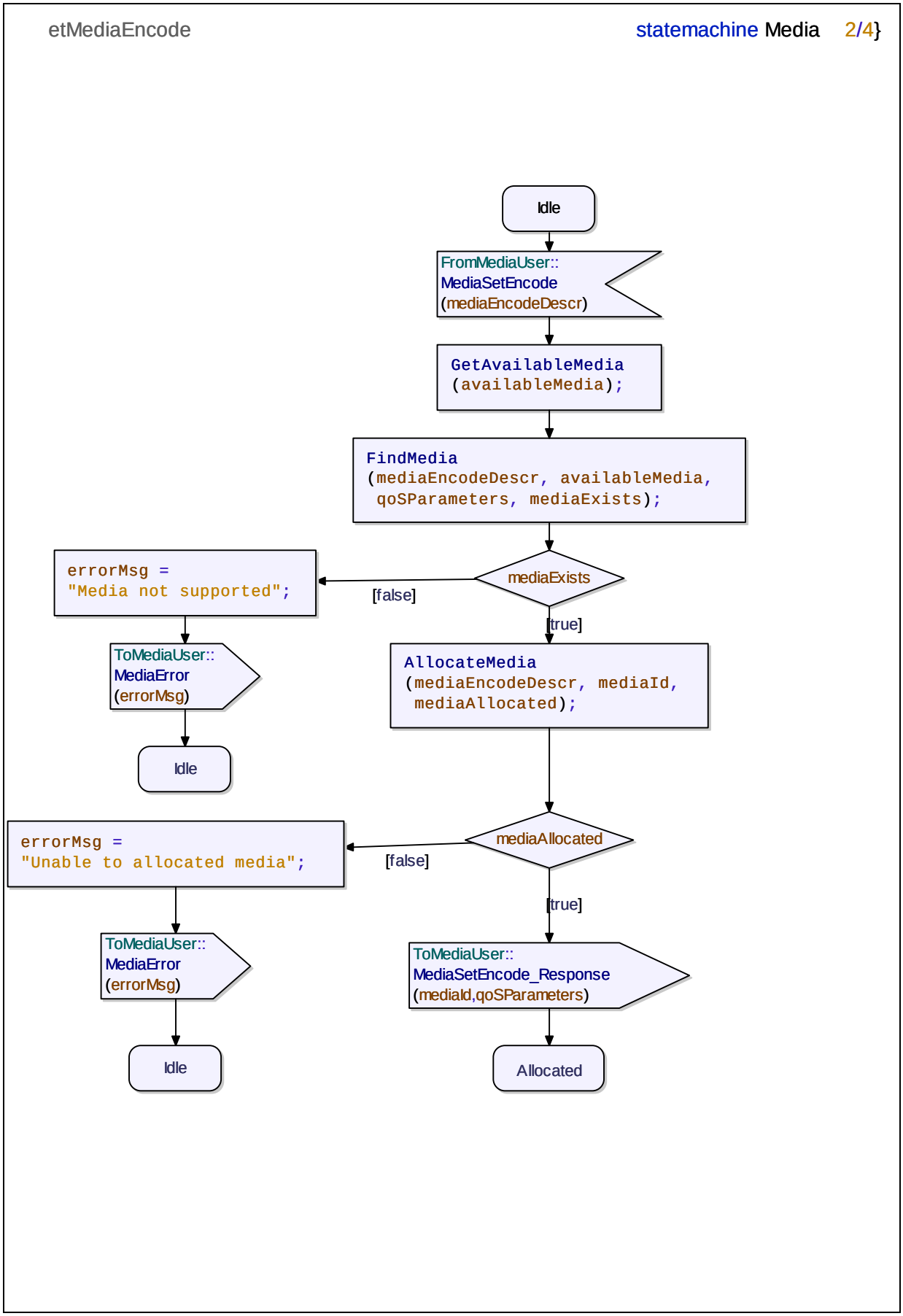


Figure 11: The *Set media encode* service capability

5.4 Message group

5.4.1 Addition to data types

The message group does not have any EPTS specific additions.

The messaging service is considered a "store and forward" service in the application plane. Any capability indicating the priority of the message is considered at user to user level, i.e. the sender may flag a message as a high priority message. However, the flagging of a message as high priority does not have any affect on the treatment of message by network nodes. Therefore, no priority indicators have been added to the message related service capabilities.

5.4.2 Extension and modification to service capabilities

The core service capabilities in message do not have any EPTS specific extensions.

Annex A (informative): Key management considerations for confidentiality, integrity and authentication

A.1 Duration of Authentication session

When an EPTS user registers for the EPTS service and authenticates itself, the service provider may either register the user based on a number of parameters. These include:

- Number of calls an EPTS user can make during the authentication session.
- Time duration of the authentication session, e.g. one hour, ten days.

The user will be required to re-register before the registration expires, if the user wants to continue using the service. If the user no longer wishes to use the service, the registration will be allowed to expire.

NOTE: The authentication session may be cleared if the EPTS manager revokes the EPTS service provided to the EPTS users.

A.2 Authentication data management

Authentication data, such as passwords need to be protected and kept confidential. The policy manager may impose security requirements as to where the authentication data can be placed. The authentication data may be placed in the user profile inside or outside the network provider's domain.

A.3 Encryption of Registration and Service request data

The registration data may be encrypted to provide confidentiality. The mechanisms used to encrypt data are out side the scope of present document.

Annex B (informative): Policy considerations

Whilst details of EPTS policy are out of scope of the present document, many of the detailed technical provisions outlined in the main body of the document are affected by the policies surrounding EPTS. This annex summarizes policy issues arising from the EPTS requirements in TR 102 302-1 [1] and the main body of the present document.

B.1 Policy establishment

B.1.1 EPTS users

The users of an EPTS service may be identified as individual users, a group of users, or an organization. In the case of individual user, the service may be provided after authenticating that particular user. In case of the group or organizations, the service may be provided by authenticating the credentials of the group or organization.

B.1.2 Network priority levels

In general EPTS is defined to be treated at a higher priority than other traffic at times of congestion. The number of levels of priority to be supported in a network may be defined by the network operator. The EPTS service provider will need to know the network priority levels. This is because the network priority scheme may differ from that of the EPTS users and organizations. The private priority schemes need to be mapped to the network priority schemes.

B.1.3 Priority of user/organization

The EPTS manager must allocate priority levels to the EPTS users, so that the EPTS users can receive services from the network, according to their priority level. The priority of a user may be described in the user/organization profile in the network.

B.1.4 Applications supported

The policy may describe the applications that are available to an EPTS user. At the minimum, a voice call is required to be supported. The policy may allow other services requiring bearer types different from those of voice.

In the case of telephony service, the policy may indicate services such as:

- Incoming calls allowed or barred from any caller or a member of EPTS.
- Outgoing calls allowed or barred to any caller or a member of EPTS.

B.1.5 Identity presentation

The policy may indicate whether a user's/group's identity is to be presented to the called party, as well as the presentation of the connected line identity to the calling party. This will allow for the protection of the calling party's as well as the called party identity.

B.1.6 Location of registration

The EPTS policy may indicate that a user can register for the EPTS service from:

- any geographic area;
- specified area, including the disaster site;

- any service provider domain;
- specified service provider domain.

B.1.7 Registrar availability

The EPTS manager may, for reliability purposes, introduce more than one registrars to provide the authentication and authorization service. An EPTS user may be provided with the primary, secondary and tertiary registrar identities.

B.1.8 Queue management

Any incoming call processing may be based on pre-queuing. The highest priority calls will then be placed in the active queue, in the FIFO order.

B.2 Implementation of Policy

NOTE: It is not necessary for a user to explicitly register and initiate EPTS. The EPTS-manager may enable the EPTS service without notification to the EPTS user.

After the policy has been developed and agreed by the parties involved (EPTS manager, network operator), and the EPTS users allocated, the next step is to implement the policy.

The EPTS policy is implemented in the following entities.

B.2.1 User/Organization profile

The user or an organization will have a profile that identifies data including:

- the user/organization data;
- services available to the user/organization:
  - Voice, Data, etc.;
  - CUG, etc.;
- duration of "Authentication session"/Registration;
- priority level of user/organization;
- authentication credentials.

B.2.2 Resource manager (SpoA)

The resource manager is responsible for providing resources for the requested services. It interacts with the CC and BC functional entities to provide resources. It acts on the priority level of the user, given by the registrar, and reserves resources accordingly.

The EPTS calls may alter the behaviour of a normal call i.e. the call blocking systems behaves like a call queuing system. The resource manager manages the queues and implements the Queuing policies such as "Highest priority, first in the queue" call to be treated first.

B.2.3 EPTS users

The EPTS users may also be informed of the policies of their organization, such as under what circumstances the EPTS is to be invoked. However, this is out of scope of the present document.

Annex C (informative): Impact of EPTS on existing protocols

The system described in the present document can be used to implement the EPTS service via different standardized protocols. These standardized protocols include SIP, H.323, ISUP and BICC. These protocols have the capabilities to convey the priority levels related to a service, and the behaviour will be governed by the systems description in the present document.

The means employed by different protocols to carry priority information is given below.

C.1 SIP

There is a priority indicator in SIP which can be used to convey the priority of the call. This priority can be set either by the user or the network. The priority defined by a user is discouraged, and preferential treatment should only be provided by the network assigned priority. There is a need to add the capability to indicate that the priority level has been set up by the network. This can also be achieved by developing a network policy that ignores the user defined priority, and modifies it at the ingress node.

C.2 ISUP/BICC

ISUP has been updated with a new "Calling Party Category" type ETS. This allows a user to be identified as an authorized ETS user. The call is then treated according to the priority level of the network.

History

Document history		
V5.1.1	May 2004	Publication