International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.262

(10/2009)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

IPCablecom

Specifications for authentication in preferential telecommunications over IPCablecom2 networks

Recommendation ITU-T J.262

ITU-T

Recommendation ITU-T J.262

Specifications for authentication in preferential telecommunications over IPCablecom2 networks

Summary

Recommendation ITU-T J.262 is one of a series of Recommendations to enable support for preferential telecommunication services over IPCablecom networks. It defines the specifications for authentication in preferential telecommunications over IPCablecom2 networks. These specifications satisfy the requirements defined in Recommendation ITU-T J.260. The essential aspects of preferential telecommunications over IPCablecom2 can be grouped into two areas: prioritization and authentication. This Recommendation defines specifications for authentication only. Authentication must be utilized to prevent unauthorized use of premium services and for emergency services in IPCablecom2 that may require preferential treatment (e.g., telecommunications for disaster relief and the emergency telecommunications service).

User authentication is necessary to determine whether to authorize a request for preferential telecommunication services. This Recommendation covers only authentication and does not address which services the authenticated user is authorized to use.

Source

Recommendation ITU-T J.262 was approved on 30 October 2009 by ITU-T Study Group 9 (2009-2012) under the WTSA Resolution 1 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Page

Introduction

Emergency and disaster communications for authorized users play a vital role in the health, safety, and welfare of people in all countries. The common thread to facilitate emergency/disaster operations is the utility of assured capabilities for user-friendly preferential telecommunication services that may be realized by technical solutions and/or administrative policy. The IPCablecom infrastructure offers an important resource for assured emergency/disaster telecommunications.

Emergency and disaster situations can impact telecommunication infrastructures. Typical impacts may include congestion overload and the need to re-deploy or extend communications capabilities beyond that covered by existing infrastructures. Even when telecommunication infrastructures are not damaged by these situations, demand for telecommunication resources soar during such events. Therefore, priority mechanisms are needed so that limited bandwidth resources can be allocated to authorized emergency workers during emergency and disaster situations.

Generally, when preferential or prioritized treatment telecommunication capabilities are offered, users of the service will be authenticated and authorized. Whether authentication and authorization are required or not, as well as implementation aspects, such as databases for personal identification numbers (PIN), are national decisions. However, without authentication and authorization, preferential treatment capabilities may be subject to abuse by non-authorized individuals.

This Recommendation defines specifications stemming from the requirements of Recommendation ITU-T J.260 for mechanisms to provide authentication in IPCablecom2 networks in support of preferential telecommunication services that need or benefit from preferential treatment.

Recommendation ITU-T J.262

Specifications for authentication in preferential telecommunications over IPCablecom2 networks

1 Scope

This Recommendation is one of a series of Recommendations to enable support for preferential telecommunication services over IPCablecom networks. These specifications do not apply to ordinary emergency calls such as people calling the police, the fire department, ambulances, etc.

Aspects of preferential telecommunications include provisions for authentication and priority (special handling). The objective of this Recommendation is to provide an initial set of authentication specifications for preferential telecommunications within IPCablecom2 networks according to the framework described in [ITU-T J.261]. This Recommendation defines specifications for capabilities, which, when implemented should help support preferential treatment telecommunication services.

NOTE – Pre-emption specifications and authorization specifications are outside the scope of this Recommendation and are considered to be national matters.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T J.260] Recommendation ITU-T J.260 (2005), *Requirements for preferential telecommunications over IPCablecom networks*.

[ITU-T J.261] Recommendation ITU-T J.261 (2009), *Framework for implementing preferential telecommunications in IPCablecom and IPCablecom2 networks*.

[ITU-T J.360] Recommendation ITU-T J.360 (2006), *IPCablecom2 architecture framework*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 assured capabilities [ITU-T J.260]: Capabilities providing high confidence or certainty that critical telecommunications are available and perform reliably.

3.1.2 authentication [ITU-T J.260]: The act or method used to verify a claimed identity.

3.1.3 authorization [ITU-T J.260]: The act of determining if a particular privilege, such as access to telecommunications resources, can be granted to the presenter of a particular credential.

3.1.4 emergency situation [ITU-T J.260]: A situation, of serious nature, that develops suddenly and unexpectedly. Extensive immediate important efforts, facilitated by telecommunications, may be required to restore a state of normality to avoid further risk to people or property. If this situation escalates, it may become a crisis and/or disaster.

3.1.5 international emergency situation [ITU-T J.260]: An emergency situation, across international boundaries, that affects more than one country.

3.1.6 label [ITU-T J.260]: An identifier occurring within or attached to data elements. In the context of preferential telecommunications it is an indication of priority. This identifier can be used as a mapping mechanism between different network priority levels.

3.1.7 policy [ITU-T J.260]: Rules (or methods) for allocating telecommunications network resources among types of traffic that may be differentiated by labels.

3.1.8 preferential [ITU-T J.260]: A capability offering advantage over regular capabilities.

3.1.9 priority treatment capabilities [ITU-T J.260]: Capabilities that provide premium access to, and/or use of telecommunications network resources.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 factor: A factor, as used in the process of authentication, represents either something known (such as a PIN, password or passphrase), something possessed (such as a card with a magnetic stripe or a security token) or something unique (such as a finger or voice print) about the individual whose identity is be authenticated.

4 Abbreviations

This Recommendation uses the following abbreviations:

AS	Application Server
CM	Cable Modem
HSS	Home Subscriber Server
ISTP	Internet Signalling Transport Protocol
MTA	Media Terminal Adapter
P-CSCF	Proxy Call Session Control Function
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
S-CSCF	Serving Call Session Control Function
SIP	Session Initiation Protocol
UA	User Agent

5 Conventions

None.

6 Authentication in IPCablecom2

Authentication in IPCablecom2 networks is impacted by two dimensions:

- location of originating and terminating devices or VoIP user agent (UA) functionality; and
- form of identity presented by the preferential telecommunication service requester and manner by which the asserted identity is verified.

Authentication entails receiving identification and identity verification/validation information necessary, prior to authorizing completion of a preferential priority call or session. This capability should exist on the access network and it must also be propagated throughout all relevant network entities to provide, as much as possible, end-to-end preferential treatment. The manner in which end-to-end preferential treatment is provided is outside the scope of this Recommendation.

The following four possibilities are to be considered for calls that require preferential treatment:

1) Originate from a UA at a location authorized for preferential treatment services and terminate at a UA at any general location.
2) Originate from a UA at a location authorized for preferential treatment services and terminate at a UA at a location that is authorized for preferential treatment services.
3) Originate from a UA at a general location and terminate at a UA at a location authorized for preferential treatment services.
4) Originate from a UA at a general location and terminate at a UA at any general location.

Authentication itself can be subdivided into two (or sometimes three) components: The first is receipt of identification information, which identifies the preferential service requester. The second is receipt of identification verification information that allows the network to verify the accuracy of the requester's claimed identity when placing a preferential service call, so that the information can be propagated to all relevant entities in the network, should the call be authorized. The third component, necessary in some situations, may require validating the identity against a database of authenticated identities.

Another factor that can impact authentication is whether preferential treatment for access will be authorized on a:

- per call basis, or a
- subscription basis.

Currently, identification and authentication are combined through the use of a personal identification number (PIN) presented by the caller after dialling an access number for enabling preferential treatment. This PIN may be validated against a PIN database to determine authorized services. PIN based authentication actually authenticates the requester, not the device being used when making the request, and thus allows preferential treatment requests to be initiated from any device. Also, this approach allows calls that require preferential treatment to be originated from circuit switched telephone devices attached to private PBX systems. The PIN based authentication approach was designed specifically for per call requests. IPCablecom2-enabled infrastructures should accommodate this legacy approach along with providing other forms of identification and authentication for VoIP-based calls using the session initiation protocol (SIP).

Appendix III of [ITU-T J.360] and [b-ITU-T J.366.8] include the three SIP authentication mechanisms specified in [b-IETF RFC 3261]:

- usage of HTTP authentication (section 22), also referred to as Digest Authentication;
- usage of transport layer security (section 26.2.1), based on TLS; and
- usage of network layer security (section 26.2.1), based on IPsec.

Identification of the calling and called party in IPCablecom2 networks is supported by SIP registration. Authentication of the called party is supported for services requiring preferential treatment by including a PIN with SIP digest or SIP over TLS or SIP over IPSec mechanisms.

6.1 IPCablecom2 PIN authentication of VoIP UA preferential treatment call to PSTN

SIP user agent (UA) functions have to register with the IMS call processing function of the service provider so they can place and receive SIP signalled calls regardless of call type. Figure 1 depicts a PIN authenticated preferential treatment request between a VoIP SIP UA and a device on the PSTN where the requester calls a specific telephone number associated with a preferential treatment application server function. For the registration of both the calling UA, and the called UA, and preferential treatment PIN authentication, the following basic steps occur (a number of acknowledgements and other secondary messages are not shown or addressed). Even though registration message exchanges are not specific to preferential treatment, they are included to provide the complete flow:

1) The calling UA sends a REGISTER message to its serving P-CSCF, the same as in (1) in Figure III.4 of [ITU-T J.360].

2) The P-CSCF performs the same activity as in (2) in Figure III.4 of [ITU-T J.360].

3) The S-CSCF creates and sends a 401 (Unauthorized) response, the same as in (5) in Figure III.4 of [ITU-T J.360].

4) The P-CSCF performs the same activities and sends the 401 (Unauthorized) response, as in (6) in Figure III.4 of [ITU-T J.360].

5) The calling UA performs the same actions as in (7) in Figure III. 4 of [ITU-T J.360].

6) The P-CSCF performs the same activities to the REGISTER message as in (8) in Figure III.4 of [ITU-T J.360].

7) The S-CSCF performs the same activities and responds with a 200 OK, as in (11) in Figure III. 4 of [ITU-T J.360].

8) The P-CSCF forwards the 200 OK, the same as in (12) in Figure III.4 of [ITU-T J.360].

9) The calling UA sends an INVITE message that is routed to the application server function for preferential treatment services (PrefTreat-AS) responsible for initiating user authentication. This may involve the user entering a special telephone number that was provided with the PIN.

10) The preferential treatment AS sends an INVITE message to a media server (PrefTreat-MS) function that will collect the user's PIN and destination UA.

11) The PrefTreat-MS Sends a 200 OK message to the PrefTreat-AS.

12) The PrefTreat-AS sends a 200 OK to the calling UA.

13) The calling UA and the PrefTreat-MS are now able to exchange RTP media to collect the user's PIN and destination UA information entered by the user.

14) The PrefTreat-MS passes the collected user PIN and destination UA to the PrefTreat-AS.

15) The PrefTreat-AS sends a message to the authentication (PrefTreat-A) function that will verify whether the supplied user PIN is valid.

16) The authentication function will validate the PIN against the authorized set of services and inform the PrefTreat-AS whether the user is a valid user to originate preferential treatment calls. Another approach is to inform the PrefTreat-AS the authorized services for that user and PrefTreat-AS determines if the requested service is included in that list.

17) The PrefTreat-AS sends a reINVITE to the calling UA.

18) The PrefTreat-AS releases the PrefTreat-MS with a BYE message.

19) The calling UA sends a 200 OK to the PrefTreat-AS.

20) The PrefTreat-MS sends a 200 OK to the PrefTreat-AS.

21) The PrefTreat-AS sends an INVITE to the provider signalling gateway (SG) to signal into the PSTN.

22) The SG sends a 200 OK to the PrefTreat-AS.

23) The PrefTreat-AS sends a reINVITE to the calling UA.

24) The calling UA sends a 200 OK to the PrefTreat-AS.

25) The calling UA and a PSTN telephone now have a preferential treatment call established and can exchange information that will be converted between RTP media and digitized analogue formats.

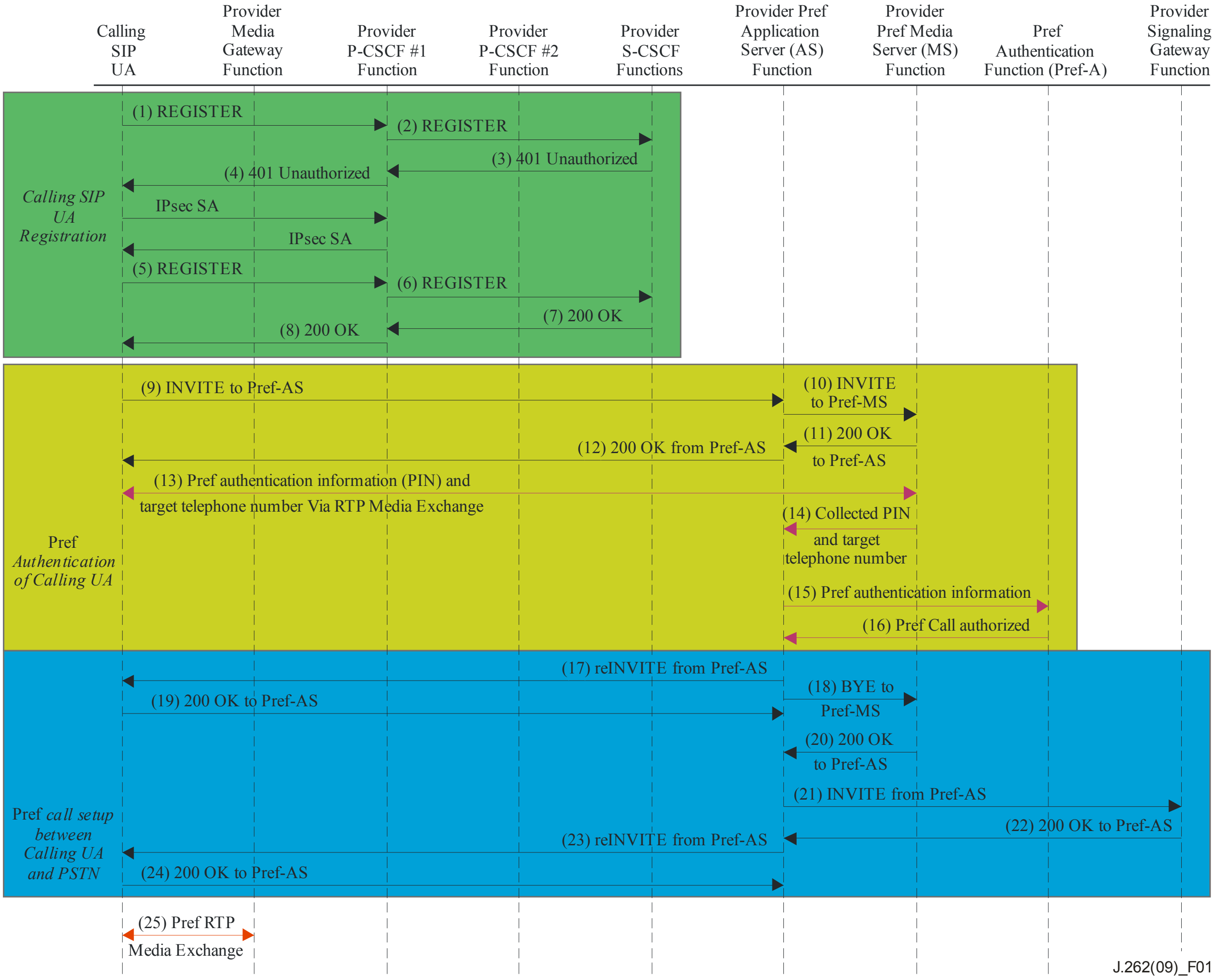
Calling SIP UA
Provider Media Gateway Function
Provider P-CSCF #1 Function
Provider P-CSCF #2 Function
Provider S-CSCF Functions
Provider Pref Application Server (AS) Function
Provider Pref Media Server (MS) Function
Pref Authentication Function (Pref-A)
Provider Signaling Gateway Function
Calling SIP UA Registration
(1) REGISTER
(2) REGISTER
(3) 401 Unauthorized
(4) 401 Unauthorized
IPsec SA
IPsec SA
(5) REGISTER
(6) REGISTER
(7) 200 OK
(8) 200 OK
Pref Authentication of Calling UA
(9) INVITE to Pref-AS
(10) INVITE to Pref-MS
(11) 200 OK to Pref-AS
(12) 200 OK from Pref-AS
(13) Pref authentication information (PIN) and target telephone number Via RTP Media Exchange
(14) Collected PIN and target telephone number
(15) Pref authentication information
(16) Pref Call authorized
Pref call setup between Calling UA and PSTN
(17) reINVITE from Pref-AS
(18) BYE to Pref-MS
(19) 200 OK to Pref-AS
(20) 200 OK to Pref-AS
(21) INVITE from Pref-AS
(22) 200 OK to Pref-AS
(23) reINVITE from Pref-AS
(24) 200 OK to Pref-AS
(25) Pref RTP Media Exchange
J.262(09)_F01

Figure 1 – VoIP preferential treatment using PIN authentication message flow

6.2 IPCablecom2 PIN authentication of VoIP UA call to VoIP UA

SIP user agent (UA) functions have to register with the IMS call processing function of the service provider so that they can place and receive SIP signalled calls regardless of call type. Figure 2 depicts a PIN authenticated preferential treatment request between two VoIP SIP UAs, where the requester of the preferential treatment calls a special telephone number associated with a preferential treatment application server function. For the registration of both the calling UA and the called UA, and PIN authentication, the following basic steps occur (a number of acknowledgements and other secondary messages are not shown or addressed). Even though registration message exchanges are not specific to preferential treatment, they are included to provide the complete flow:

1) The calling UA sends a REGISTER message to its serving P-CSCF, the same as in (1) in Figure III.4 of [ITU-T J.360].

2) The P-CSCF performs the same activity as in (2) in Figure III.4 of [ITU-T J.360].

3) The S-CSCF creates and sends a 401 (Unauthorized) response, the same as in (5) in Figure III.4 of [ITU-T J.360].

4) The P-CSCF performs the same activities to the 401 (Unauthorized) response as in (6) in Figure III.4 of [ITU-T J.360].

5) The calling UA performs the same actions as in (7) in Figure III.4 of [ITU-T J.360].

6) The P-CSCF performs the same activities to the REGISTER message as in (8) in Figure III.4 of [ITU-T J.360].

7) The S-CSCF performs the same activities and responds with a 200 OK, as in (11) in Figure III.4 of [ITU-T J.360].

8) The P-CSCF forwards the 200 OK, the same as in (12) in Figure III.4 of [ITU-T J.360].

9) The same as step 1 above, but between the called UA and its serving P-CSCF.

10) The same as step 2 above, but between the called UA's serving P-CSCF and the S-CSCF.

11) The same as step 3 above, but between the called UA's serving P-CSCF and the S-CSCF.

12) The same as step 4 above, but between the called UA and its serving P-CSCF.

13) The same as step 5 above, but between the called UA and its serving P-CSCF.

14) The same as step 6 above, but between the called UA's serving P-CSCF and the S-CSCF.

15) The same as step 7 above, but between the called UA's serving P-CSCF and the S-CSCF.

16) The same as step 8 above, but between the called UA and its serving P-CSCF.

17) The calling UA sends an INVITE message that is routed to the PrefTreat application server (PrefTreat-AS) function that is responsible for initiating user authentication.

18) The PrefTreat-AS sends an INVITE message to a PrefTreat media server (PrefTreat-MS) function that will collect the user PIN and destination UA.

19) The PrefTreat-MS Sends a 200 OK message to the PrefTreat-AS.

20) The PrefTreat-AS sends a 200 OK to the calling UA.

21) The calling UA and the PrefTreat-MS are now able to exchange RTP media to collect the user PIN and destination UA information entered by the calling user.

22) PrefTreat-MS passes the collected user PIN and destination UA to the PrefTreat-AS.

23) The PrefTreat-AS sends a message to the PrefTreat authentication (PrefTreat-A) functions that will verify if the supplied user PIN is valid. Another approach is to inform the PrefTreat-AS the authorized services for that user and PrefTreat-AS determines if the requested service is included in that list.

24) The PrefTreat-A will inform the PrefTreat-AS whether the user is authorized to originate preferential treatment service.

25) The PrefTreat-AS sends a reINVITE to the calling UA.

26) The PrefTreat-AS releases the PrefTreat-MS with a BYE message.

27) The calling UA sends a 200 OK to the PrefTreat-AS.

28) The PrefTreat-MS sends a 200 OK to the PrefTreat-AS.

29) The PrefTreat-AS sends an INVITE to the called UA.

30) The called UA sends a 200 OK to the PrefTreat-AS.

31) The PrefTreat-AS sends a reINVITE to the calling UA.

32) The calling UA sends a 200 OK to the PrefTreat-AS.

33) The calling and called UAs now have a preferential treatment call established and can exchange RTP media.

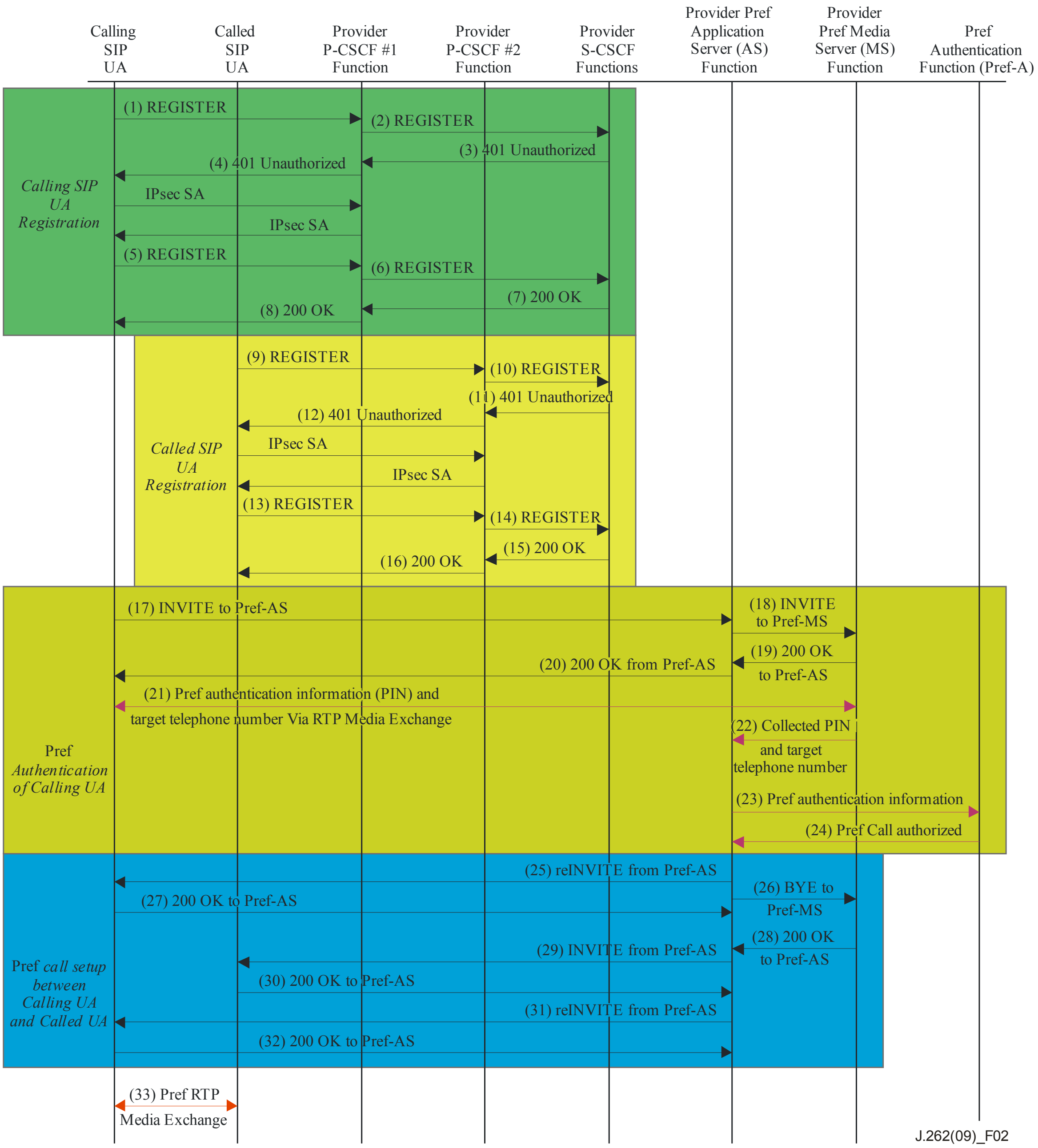
Calling SIP UA
Called SIP UA
Provider P-CSCF #1 Function
Provider P-CSCF #2 Function
Provider S-CSCF Functions
Provider Pref Application Server (AS) Function
Provider Pref Media Server (MS) Function
Pref Authentication Function (Pref-A)
Calling SIP UA Registration
(1) REGISTER
(2) REGISTER
(3) 401 Unauthorized
(4) 401 Unauthorized
IPsec SA
IPsec SA
(5) REGISTER
(6) REGISTER
(7) 200 OK
(8) 200 OK
Called SIP UA Registration
(9) REGISTER
(10) REGISTER
(11) 401 Unauthorized
(12) 401 Unauthorized
IPsec SA
IPsec SA
(13) REGISTER
(14) REGISTER
(15) 200 OK
(16) 200 OK
Pref Authentication of Calling UA
(17) INVITE to Pref-AS
(18) INVITE to Pref-MS
(19) 200 OK to Pref-AS
(20) 200 OK from Pref-AS
(21) Pref authentication information (PIN) and target telephone number Via RTP Media Exchange
(22) Collected PIN and target telephone number
(23) Pref authentication information
(24) Pref Call authorized
Pref call setup between Calling UA and Called UA
(25) reINVITE from Pref-AS
(26) BYE to Pref-MS
(27) 200 OK to Pref-AS
(28) 200 OK to Pref-AS
(29) INVITE from Pref-AS
(30) 200 OK to Pref-AS
(31) reINVITE from Pref-AS
(32) 200 OK to Pref-AS
(33) Pref RTP Media Exchange
J.262(09)_F02

Figure 2 – VoIP preferential treatment service PIN authentication message flow

6.3 IPCablecom2 preferential treatment services subscription authentication in VoIP UA to VoIP UA calls – Priority signalled by the UA using R-P header in the INVITE message

SIP user agent (UA) functions have to register with the IMS call processing function of the service provider so that they can place and receive SIP signalled calls regardless of call type. Figure 3 depicts a subscription authenticated preferential treatment request between two VoIP SIP UAs, where the requester calls a special telephone number associated with a preferential treatment service application server function. For registration of both the calling UA and the called UA, and PIN authentication for preferential treatment, the following basic steps occur (a number of acknowledgements and other secondary messages are not shown or addressed). Even though registration message exchanges are not specific to preferential treatment, they are included to provide the complete flow:

1) The calling UA sends a REGISTER message to its serving P-CSCF, the same as in (1) in Figure III.4 of [ITU-T J.360].

2) The P-CSCF performs the same activity as in (2) in Figure III.4 of [ITU-T J.360].

3) The S-CSCF creates and sends a 401 (Unauthorized) response, the same as in (5) in Figure III.4 of [ITU-T J.360].

4) The P-CSCF performs the same activities to the 401 (Unauthorized) response as in (6) in Figure III.4 of [ITU-T J.360].

5) The calling UA performs the same actions as in (7) in Figure III.4 of [ITU-T J.360].

6) The P-CSCF performs the same activities to the REGISTER message as in (8) in Figure III.4 of [ITU-T J.360].

7) The S-CSCF performs the same activities and responds with a 200 OK, as in (11) in Figure III.4 of [ITU-T J.360].

8) The P-CSCF forwards the 200 OK, the same as in (12) in Figure III.4 of [ITU-T J.360].

9) The same as step 1 above, but between the called UA and its serving P-CSCF.

10) The same as step 2 above, but between the called UA's serving P-CSCF and the S-CSCF.

11) The same as step 3 above, but between the called UA's serving P-CSCF and the S-CSCF.

12) The same as step 4 above, but between the called UA and its serving P-CSCF.

13) The same as step 5 above, but between the called UA and its serving P-CSCF.

14) The same as step 6 above, but between the called UA's serving P-CSCF and the S-CSCF.

15) The same as step 7 above, but between the called UA's serving P-CSCF and the S-CSCF.

16) The same as step 8 above, but between the called UA and its serving P-CSCF.

17) The calling UA sends an INVITE message that is routed to the S-CSCF. The INVITE includes an R-P header indicating priority treatment.

18) The S-CSCF queries the HSS to determine if the calling UA is authorized to place a preferential treatment service call.

19) The HSS responds to the S-CSCF either authorizing (acknowledgement) or not authorizing.

20) The S-CSCF sends an INVITE to the called UA's serving P-CSCF.

21) The called UA's serving P-CSCF forwards the INVITE to the called UA.

22) The called UA sends a 200 OK to the S-CSCF.

23) The S-CSCF sends a 200 OK to the calling UA's serving P-CSCF.

24) The calling UA's serving P-CSCF sends a 200 OK to the calling UA.

25) The calling and called UAs now have a preferential treatment call established and can exchange RTP media.

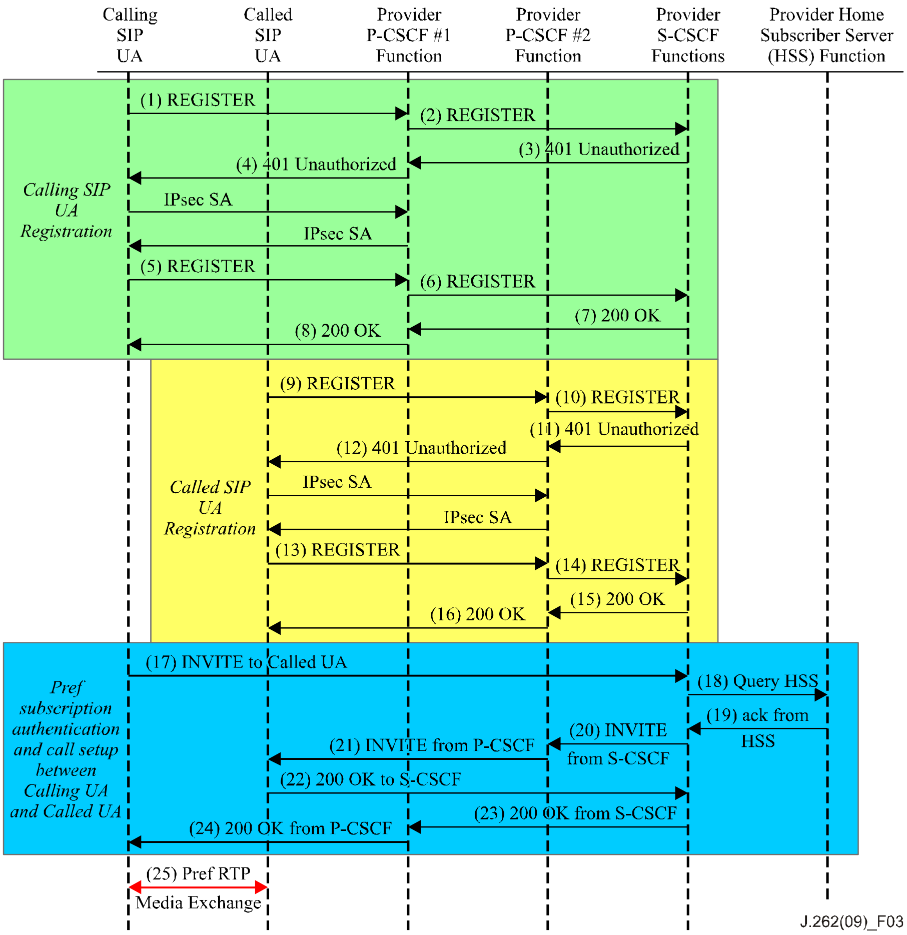

Figure 3 – VoIP subscription authentication message flow – Priority signalled by the UA, using R-P header in the INVITE message

6.4 IPCablecom2 preferential treatment services subscription authentication in VoIP UA to VoIP UA Calls – Priority signalled by the UA, using an identifier

There are two options defined in [b-ITU-T J.263] to indicate that a call is to be given preferential treatment. In this clause the UA sends an identifier, which is included as a trigger, in the initial filter criteria contained in the user profile. The call flow is the same as in Figure 3, except for the following steps. After step 6, where the P-CSCF sends a REGISTER message to the S-CSCF, a request is sent to the HSS to retrieve the user profile, and not when the INVITE is received in Step 18. The HSS returns the initial filter criteria for the user, which includes enabling the detection of identifiers (for example, a feature code along with a special destination number or a special access number with PIN are defined) for determining that the user is requesting a preferential treatment call. Steps 18 and 19 are performed during registration and not after the INVITE message is initiated in step 17. The initial filter criterion is used to determine the preferential treatment application server to which the INVITE request is forwarded. In step 17, the INVITE includes the identifier in the SDP instead of the R-P header of the previous case. The identifier triggers the preferential treatment processing at the P-CSCF, where the R-P header is inserted with the appropriate priority value as discussed in [b-ITU-T J.263].

1) The calling UA sends a REGISTER message to its serving P-CSCF, the same as in (1) in Figure III.4 of [ITU-T J.360]. This message contains an identifier indicating a preferential telecommunications service user.

2) The P-CSCF performs the same activity as in (2) in Figure III.4 of [ITU-T J.360].

3) The S-CSCF creates and sends a 401 (Unauthorized) response, the same as in (5) in Figure III.4 of [ITU-T J.360].

4) The P-CSCF performs the same activities to the 401 (Unauthorized) response as in (6) in Figure III.4 of [ITU-T J.360].

5) The calling UA performs the same actions as in (7) in Figure III.4 of [ITU-T J.360].

6) The P-CSCF performs the same activities to the REGISTER message as in (8) in Figure III.4 of [ITU-T J.360].

7) The S-CSCF queries the HSS to determine if the calling UA is authorized to place a preferential treatment service call.

8) The HSS returns either the initial filter criteria for the user, if authorized, that includes enabling the detection of identifiers (for example, a feature code along with special destination number or special access number with PIN are defined) for determining that the user is requesting a preferential treatment call, or it returns "not authorized".

9) The S-CSCF responds with a 200 OK, the same as in (11) in Figure III.4 of [ITU-T J.360].

10) The P-CSCF forwards the 200 OK, the same as in (12) in Figure III.4 of [ITU-T J.360].

11) The same as step 1 above, but between the called UA and its serving P-CSCF.

12) The same as step 2 above, but between the called UA's serving P-CSCF and the S-CSCF.

13) The same as step 3 above, but between the called UA's serving P-CSCF and the S-CSCF.

14) The same as step 4 above, but between the called UA and its serving P-CSCF.

15) The same as step 5 above, but between the called UA and its serving P-CSCF.

16) The same as step 6 above, but between the called UA's serving P-CSCF and the S-CSCF.

17) The same as step 9 above, but between the called UA's serving P-CSCF and the S-CSCF.

18) The same as step 10 above, but between the called UA and its serving P-CSCF.

19) The calling UA sends an INVITE message with the preferential user identifier, which is routed to the S-CSCF.

20) The S-CSCF sends an INVITE to the called UA's serving P-CSCF.

21) The called UA's serving P-CSCF forwards the INVITE to the called UA.

22) The called UA sends a 200 OK to the S-CSCF.

23) The S-CSCF sends a 200 OK to the calling UA's serving P-CSCF.

24) The calling UA's serving P-CSCF sends a 200 OK to the calling UA.

25) The calling and called UAs now have a preferential treatment call established and can exchange RTP media.

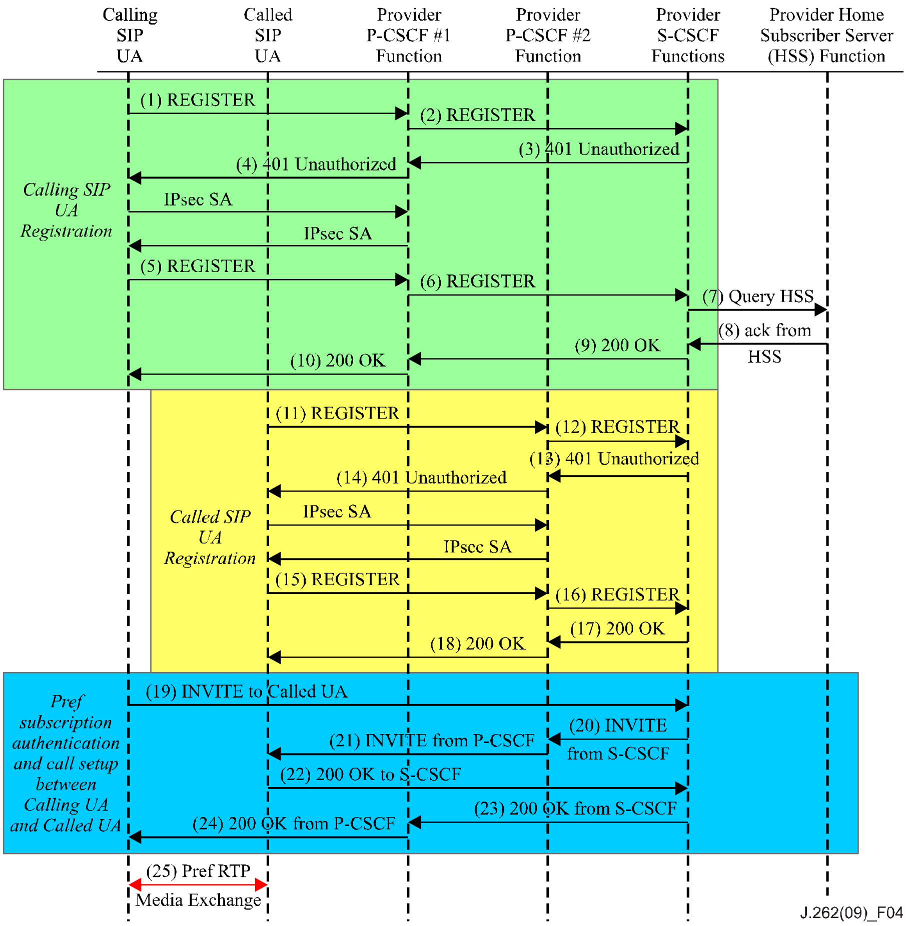

Figure 4 – VoIP subscription authentication message flow – Priority signalled by the UA, using an identifier

7 IPCablecom2 preferential telecommunication services authentication requirements

The following are specific requirements for authentication of preferential telecommunications sessions within the IPCablecom2 architecture.

If used in the UEs, they must be able to securely store usernames and passwords in a manner that minimizes risk. If this approach is used, the UE should prompt users for username and password.

Bibliography

[b-ITU-T E.106] Recommendation ITU-T E.106 (2003), *International Emergency Preference Scheme (IEPS) for disaster relief operations*.

[b-ITU-T J.263] Recommendation ITU-T J.263 (2009), *Specification for priority in preferential telecommunications over IPCablecom2 networks.*

[b-ITU-T J.366.8] Recommendation ITU-T J.366.8 (2006), *IPCablecom2 IP Multimedia Subsystem (IMS); Network domain security specification*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T Y.1271] Recommendation ITU-T Y.1271 (2004), *Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks*.

[b-ITU-T Y.2205] Recommendation ITU-T Y.2205 (2008), *Next Generation Networks – Emergency telecommunications – Technical considerations*.

[b-ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.

[b-IETF RFC 2560] IETF RFC 2560 (1999), *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.*

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS).*

[b-IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol.*

[b-IETF RFC 3550] IETF RFC 3550 (2003), *Transport protocol for Real-Time Applications.*

[b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol.*

[b-IETF RFC 4120] IETF RFC 4120 (2005), *The Kerberos Network Authentication Service (V5).*

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*.

[b-IETF RFC 4302] IETF RFC 4302 (2005), *IP Authentication Header*.

[b-IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP).*

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol*.

[b-IETF RFC 4346] IETF RFC 4346 (2006), *The Transport Layer Security (TLS) Protocol Version 1.1*.

[b-IETF RFC 4513] IETF RFC 4513 (2006), *Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Cable networks and transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2010