

Union internationale des télécommunications

**UIT-T**

SECTEUR DE LA NORMALISATION  
DES TÉLÉCOMMUNICATIONS  
DE L'UIT

**J.262**

(10/2009)

SÉRIE J: RÉSEAUX CÂBLÉS ET TRANSMISSION DES  
SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET  
AUTRES SIGNAUX MULTIMÉDIAS

IPCablecom

---

**Spécifications relatives à l'authentification pour  
les télécommunications à traitement préférentiel  
sur les réseaux IPCablecom2**

Recommandation UIT-T J.262





## Recommandation UIT-T J.262

### Spécifications relatives à l'authentification pour les télécommunications à traitement préférentiel sur les réseaux IPCom2

#### Résumé

La Recommandation UIT-T J.262 fait partie d'une série de Recommandations permettant de prendre en charge les services de télécommunication à traitement préférentiel sur les réseaux IPCom. Elle définit les spécifications relatives à l'authentification des télécommunications à traitement préférentiel sur les réseaux IPCom2. Ces spécifications sont conformes aux prescriptions contenues dans la Recommandation UIT-T J.260. Les principaux aspects des télécommunications à traitement préférentiel sur les réseaux IPCom2 peuvent être regroupés en deux domaines: la hiérarchisation des priorités et l'authentification. Cette Recommandation définit uniquement les spécifications relatives à l'authentification. L'authentification doit être utilisée pour empêcher l'utilisation non autorisée des services kiosques et des services d'urgence sur les réseaux IPCom2 pouvant nécessiter un traitement préférentiel (par exemple: télécommunications pour les secours en cas de catastrophe et services de télécommunications d'urgence).

L'authentification de l'utilisateur est nécessaire pour déterminer s'il faut accéder à une demande de services de télécommunication à traitement préférentiel. Cette Recommandation porte uniquement sur l'authentification et ne traite pas des services que l'utilisateur authentifié est autorisé à utiliser.

#### Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T J.262	2009-10-30	9

## AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

## NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

## DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous <http://www.itu.int/ITU-T/ipr/>.

© UIT 2010

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

## TABLE DES MATIÈRES

	<b>Page</b>
1	Domaine d'application ..... 1
2	Références..... 1
3	Définitions ..... 1
3.1	Termes définis dans d'autres documents ..... 1
3.2	Termes définis dans la présente Recommandation ..... 2
4	Abréviations..... 2
5	Conventions ..... 2
6	Authentification dans les réseaux IPCablecom2 ..... 3
6.1	Authentification par numéro PIN dans les réseaux IPCablecom2 –Appel à traitement préférentiel d'un agent d'utilisateur de VoIP au RTPC ..... 4
6.2	Authentification par numéro PIN dans les réseaux IPCablecom2 –Appel entre deux agents d'utilisateur de VoIP ..... 6
6.3	Authentification fondée sur un abonnement aux services à traitement préférentiel dans les réseaux IPCablecom2 – Appels entre deux agents d'utilisateur de VoIP – Priorité signalée par l'agent d'utilisateur au moyen de l'en-tête R-P dans le message INVITE ..... 8
6.4	Authentification fondée sur un abonnement aux services à traitement préférentiel dans les réseaux IPCablecom2 – Appels entre deux agents d'utilisateur de VoIP – Priorité signalée par l'agent d'utilisateur au moyen d'un identificateur ..... 10
7	Prescriptions d'authentification pour les services de télécommunication à traitement préférentiel dans les réseaux IPCablecom2 ..... 12
	Bibliographie..... 13

## **Introduction**

Les télécommunications en cas d'urgence et de catastrophe pour les utilisateurs autorisés sont d'une importance vitale pour la santé, la sécurité et le bien-être de la population dans tous les pays. Habituellement, pour faciliter les opérations en cas d'urgence et de catastrophe, on utilise des capacités garanties pour la fourniture de services de télécommunication à traitement préférentiel faciles à utiliser, ces capacités pouvant être assurées par des solutions techniques ou par une politique administrative. L'infrastructure IPCablecom constitue une ressource importante pour prendre en charge des services garantis de télécommunication en cas d'urgence et de catastrophe.

Les situations d'urgence et de catastrophe peuvent avoir une incidence sur les infrastructures de télécommunication, par exemple des surcharges et des encombrements peuvent se produire et il peut être nécessaire de redéployer ou d'étendre les capacités de communication au-delà des capacités offertes par les infrastructures existantes. Même lorsque les infrastructures de télécommunication ne sont pas endommagées, la demande de ressources de télécommunication explose dans ce type de situation. Par conséquent, des mécanismes de hiérarchisation des priorités sont nécessaires pour que les ressources de largeur de bande limitées puissent être attribuées aux secouristes autorisés dans les situations d'urgence et de catastrophe.

D'une manière générale, lorsqu'un service de télécommunication à traitement préférentiel ou bénéficiant de la priorité sera offert, les utilisateurs du service seront authentifiés et autorisés. La nécessité ou non d'une authentification et d'une autorisation ainsi que les aspects relatifs à la mise en œuvre, par exemple les bases de données pour les numéros d'identification personnels (PIN), relèvent de décisions nationales. Toutefois, sans authentification ni autorisation, les capacités de traitement préférentiel peuvent faire l'objet d'utilisations abusives de la part d'individus non autorisés.

La présente Recommandation définit des spécifications découlant des prescriptions énoncées dans la Recommandation UIT-T J.260 concernant les mécanismes d'authentification dans les réseaux IPCablecom<sup>2</sup> pour la prise en charge de services de télécommunication à traitement préférentiel.

## Recommandation UIT-T J.262

### Spécifications relatives à l'authentification pour les télécommunications à traitement préférentiel sur les réseaux IPCablecom2

#### 1 Domaine d'application

La présente Recommandation fait partie d'une série de Recommandations permettant de prendre en charge les services de télécommunication à traitement préférentiel sur les réseaux IPCablecom. Ces spécifications ne s'appliquent pas aux appels d'urgence ordinaires (destinés à la police, aux pompiers, aux ambulanciers, etc.).

Les télécommunications à traitement préférentiel comportent des aspects comme l'authentification et la priorité (traitement spécial). La présente Recommandation a pour objet de fournir un ensemble initial de spécifications d'authentification pour les télécommunications à traitement préférentiel dans les réseaux IPCablecom2 conformément au cadre décrit dans le document [UIT-T J.261]. Elle spécifie des capacités qui, une fois mises en œuvre, devraient faciliter la prise en charge des services de télécommunication à traitement préférentiel.

NOTE – Les spécifications de préemption et d'autorisation sont en dehors du domaine d'application de la présente Recommandation et sont considérées comme relevant du ressort de chaque pays.

#### 2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

[UIT-T J.260] Recommandation UIT-T J.260 (2005), *Prescriptions relatives aux communications à traitement préférentiel sur les réseaux IPCablecom*.

[UIT-T J.261] Recommandation UIT-T J.261 (2009), *Cadre applicable à la mise en œuvre des télécommunications à traitement préférentiel sur les réseaux IPCablecom et IPCablecom2*.

[UIT-T J.360] Recommandation UIT-T J.360 (2006), *Architecture générale IPCablecom2*.

#### 3 Définitions

##### 3.1 Termes définis dans d'autres documents

La présente Recommandation utilise les termes suivants définis dans d'autres documents:

**3.1.1 capacités garanties** [UIT-T J.260]: capacités assurant avec une haute probabilité ou avec certitude, la fourniture et le fonctionnement fiable de communications critiques.

**3.1.2 authentification** [UIT-T J.260]: acte ou méthode appliqués pour vérifier une identité déclarée.

**3.1.3 habilitation, autorisation** [UIT-T J.260]: acte consistant à déterminer si un privilège particulier, tel que l'accès à des ressources de télécommunication, peut être accordé au détenteur d'un mandat.

**3.1.4 situation d'urgence** [UIT-T J.260]: situation grave, survenue subitement et de manière inattendue. Des efforts immédiats importants peuvent être nécessaires, facilités par les télécommunications, pour rétablir une situation normale et empêcher que les personnes ou les biens subissent de nouveaux dommages. Si la situation s'aggrave, elle peut se transformer en crise ou en catastrophe.

**3.1.5 situation d'urgence internationale** [UIT-T J.260]: situation d'urgence affectant plusieurs pays.

**3.1.6 étiquette** [UIT-T J.260]: identificateur faisant partie des éléments de données ou attachés à ceux-ci. Dans le contexte de communications à traitement préférentiel, il s'agit d'une indication de priorité. Cet identificateur peut être utilisé comme un mécanisme de mappage entre différents niveaux de priorité de réseau.

**3.1.7 politique** [UIT-T J.260]: règles (ou méthodes) de répartition des ressources du réseau de télécommunication entre différents types de trafic, éventuellement différenciés au moyen d'étiquettes.

**3.1.8 préférentiel** [UIT-T J.260]: qualifie une capacité accordant certains privilèges par rapport au service régulier.

**3.1.9 capacités de traitement prioritaire** [UIT-T J.260]: capacités permettant d'accéder aux ressources d'un réseau de télécommunication et/ou de les utiliser de manière prioritaire.

## 3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

**3.2.1 facteur**: dans le processus d'authentification, un facteur représente quelque chose de connu (par exemple un numéro PIN, un mot de passe ou une phrase de passe) par l'individu dont l'identité doit être authentifiée, quelque chose que cet individu possède (par exemple une carte avec une bande magnétique ou un jeton de sécurité) ou quelque chose d'unique (par exemple une empreinte digitale ou vocale) qui caractérise cet individu.

## 4 Abréviations

Les abréviations suivantes sont employées dans la présente Recommandation:

AS	serveur d'application ( <i>application server</i> )
CM	câblo-modem
HSS	serveur d'abonnés résidentiels ( <i>home subscriber server</i> )
ISTP	protocole de transport de signalisation Internet ( <i>Internet signalling transport protocol</i> )
MTA	adaptateur de terminal de média ( <i>media terminal adapter</i> )
P-CSCF	fonction relais de commande de session d'appel ( <i>proxy call session control function</i> )
PIN	numéro d'identification personnel ( <i>personal identification number</i> )
RTPC	réseau téléphonique public commuté
S-CSCF	fonction serveur de commande de session d'appel ( <i>servicing call session control function</i> )
SIP	protocole d'ouverture de session ( <i>session initiation protocol</i> )
UA	agent d'utilisateur ( <i>user agent</i> )

## 5 Conventions

Aucune.

## 6 Authentification dans les réseaux IPCablecom2

Dans les réseaux IPCablecom2, les deux éléments suivants ont une incidence sur l'authentification:

- emplacement des dispositifs d'origine et de destination ou de la fonctionnalité d'agent d'utilisateur (UA) de VoIP; et
- format de l'identité présentée par le demandeur du service de télécommunication à traitement préférentiel et manière dont l'identité assertée est vérifiée.

L'authentification consiste à recevoir les informations d'identification et les informations de vérification/validation d'identité nécessaires avant qu'un appel ou qu'une session à traitement préférentiel ne puisse être autorisé. Cette capacité devrait exister dans le réseau d'accès et doit également être fournie dans toutes les entités de réseau concernées pour assurer, autant que possible, un traitement préférentiel de bout en bout. La manière dont est assuré le traitement préférentiel de bout en bout sort du cadre de la présente Recommandation.

Pour les appels qui nécessitent un traitement préférentiel, il existe quatre possibilités, à savoir:

- 1) appel provenant d'un UA situé à un emplacement autorisé pour les services à traitement préférentiel et destiné à un UA situé à un emplacement général;
- 2) appel provenant d'un UA situé à un emplacement autorisé pour les services à traitement préférentiel et destiné à un UA situé à un emplacement autorisé pour les services à traitement préférentiel;
- 3) appel provenant d'un UA situé à un emplacement général et destiné à un UA situé à un emplacement autorisé pour les services à traitement préférentiel;
- 4) appel provenant d'un UA situé à un emplacement général et destiné à un UA situé à un emplacement général.

L'authentification proprement dite peut être subdivisée en deux (ou parfois trois) étapes: la première est la réception des informations d'identification du demandeur du service à traitement préférentiel. La deuxième est la réception des informations de vérification d'identification qui permettent au réseau de vérifier l'exactitude de l'identité déclarée par le demandeur lorsqu'il lance un appel de service à traitement préférentiel, afin que les informations puissent être transmises à toutes les entités concernées dans le réseau si l'appel est autorisé. La troisième étape, nécessaire dans certaines situations, est la validation de l'identité par rapport à une base de données d'identités authentifiées.

Un autre élément qui peut avoir une incidence sur l'authentification est la question de savoir si l'autorisation du traitement préférentiel pour l'accès se fait:

- pour chaque appel; ou
- pour chaque abonnement.

Actuellement, l'identification et l'authentification sont combinées et reposent sur la présentation par l'appelant d'un numéro d'identification personnel (PIN) après avoir composé un numéro d'accès afin d'activer le traitement préférentiel. Ce numéro PIN peut être validé par rapport à une base de données de numéros PIN pour déterminer les services autorisés. En réalité, l'authentification fondée sur le numéro PIN permet d'authentifier le demandeur, mais pas le dispositif utilisé pour la demande, et permet donc de lancer des demandes de traitement préférentiel depuis n'importe quel dispositif. Cette méthode permet aussi de lancer des appels nécessitant un traitement préférentiel depuis des téléphones à commutation de circuits rattachés à des systèmes PBX privés. La méthode d'authentification fondée sur le numéro PIN a été conçue expressément pour les demandes concernant un appel donné. Les infrastructures IPCablecom2 devraient prendre en charge cette méthode existante ainsi que d'autres formes d'identification et d'authentification pour les appels de VoIP utilisant le protocole d'ouverture de session (SIP).

L'Appendice III de la Recommandation [UIT-T J.360] et de la Recommandation [b-UIT-T J.366.8] incluent les trois mécanismes d'authentification SIP spécifiés dans le document [b-IETF RFC 3261]:

- utilisation de l'authentification HTTP (§ 22), également appelée authentification Digest;
- utilisation de la sécurité de couche de transport (§ 26.2.1), fondée sur le protocole TLS; et
- utilisation de la sécurité de couche de réseau (§ 26.2.1), fondée sur le protocole IPsec.

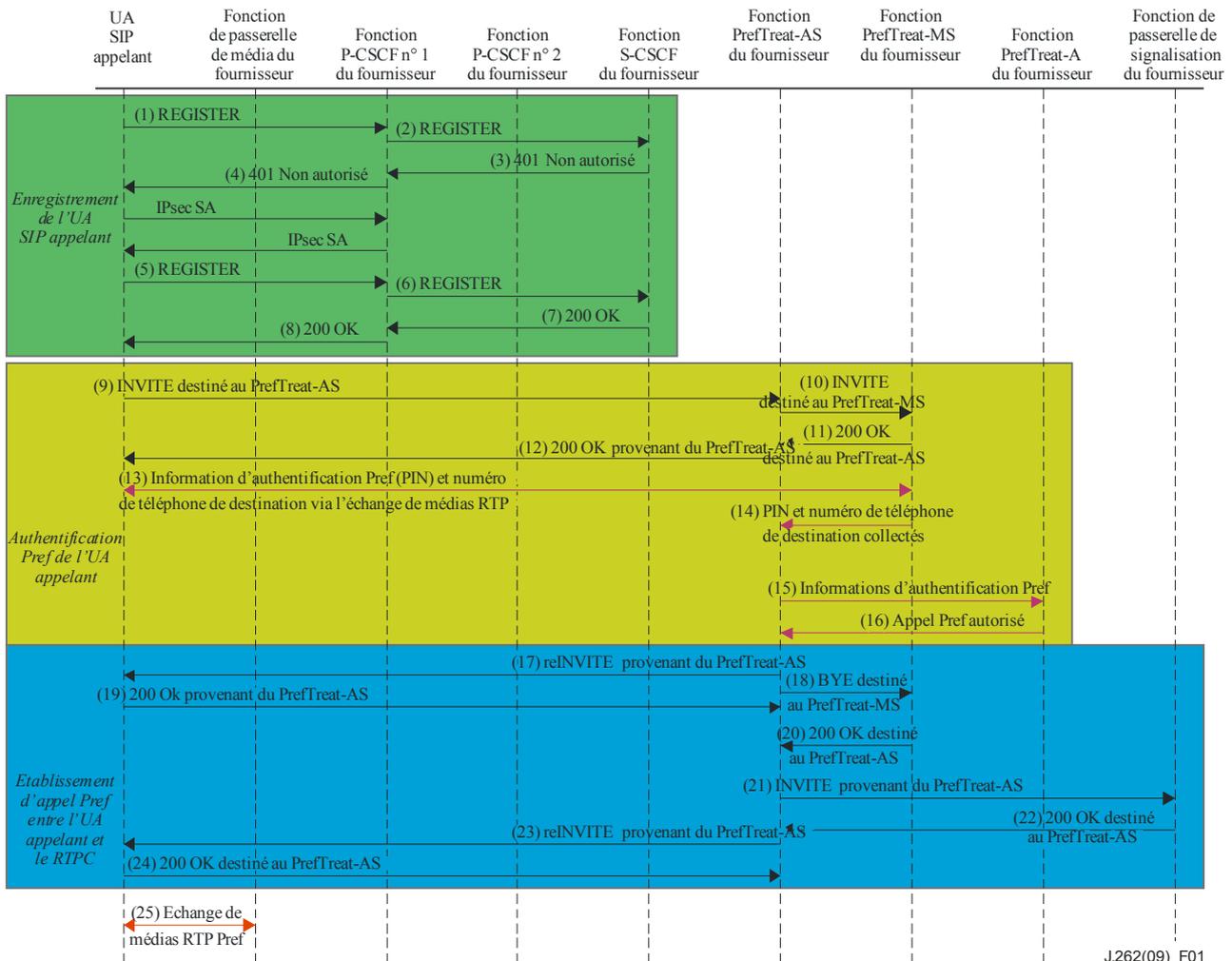
L'identification de l'appelant et de l'appelé dans les réseaux IPCablecom2 est prise en charge par l'enregistrement SIP. L'authentification de l'appelé est prise en charge pour les services nécessitant un traitement préférentiel et consiste à inclure un numéro PIN avec les mécanismes Digest SIP ou SIP sur TLS ou SIP sur IPsec.

### **6.1 Authentification par numéro PIN dans les réseaux IPCablecom2 – Appel à traitement préférentiel d'un agent d'utilisateur de VoIP au RTPC**

Les fonctions d'agent d'utilisateur (UA) SIP doivent s'enregistrer auprès de la fonction de traitement d'appel IMS du fournisseur de service de manière à pouvoir lancer et recevoir des appels à signalisation SIP indépendamment du type d'appel. La Figure 1 illustre une demande de traitement préférentiel avec authentification par numéro PIN entre un agent d'utilisateur SIP de VoIP et un dispositif sur le RTPC, pour laquelle le demandeur appelle un numéro de téléphone particulier associé à une fonction de serveur d'application pour le traitement préférentiel. Pour l'enregistrement de l'UA appelant et de l'UA appelé et l'authentification par numéro PIN pour le traitement préférentiel, les étapes de base sont les suivantes (un certain nombre d'accusés de réception et d'autres messages secondaires ne sont pas indiqués). Même si les échanges de messages d'enregistrement ne sont pas propres au traitement préférentiel, ils sont inclus afin de fournir le flux complet:

- 1) L'UA appelant envoie un message REGISTER à la fonction P-CSCF dont il relève, comme au point (1) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 2) La fonction P-CSCF réalise la même activité qu'au point (2) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 3) La fonction S-CSCF crée et envoie une réponse 401 (non autorisé), comme au point (5) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 3) La fonction P-CSCF réalise les mêmes activités et envoie la réponse 401 (non autorisé), comme au point (6) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 5) L'UA appelant réalise les mêmes actions qu'au point (7) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 6) La fonction P-CSCF réalise les mêmes activités concernant le message REGISTER qu'au point (8) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 7) La fonction S-CSCF réalise les mêmes activités et répond par un message 200 OK, comme au point (11) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 8) La fonction P-CSCF retransmet le message 200 OK, comme au point (12) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 9) L'UA appelant envoie un message INVITE qui est acheminé à la fonction de serveur d'application pour les services à traitement préférentiel (PrefTreat-AS), qui est chargée de lancer l'authentification de l'utilisateur. Pour cela, il se peut que l'utilisateur doive composer un numéro de téléphone spécial qui a été fourni avec le numéro PIN.
- 10) Le serveur PrefTreat-AS envoie un message INVITE à une fonction de serveur de média (PrefTreat-MS), qui collectera le numéro PIN de l'utilisateur et les informations relatives à l'UA de destination.

- 11) Le serveur PrefTreat-MS envoie un message 200 OK au serveur PrefTreat-AS.
- 12) Le serveur PrefTreat-AS envoie un message 200 OK à l'UA appelant.
- 13) L'UA appelant et le serveur PrefTreat-MS peuvent maintenant échanger des médias RTP en vue de la collecte du numéro PIN de l'utilisateur et des informations relatives à l'UA de destination saisis par l'utilisateur.
- 14) Le serveur PrefTreat-MS transmet au serveur PrefTreat-AS le numéro PIN de l'utilisateur et les informations relatives à l'UA de destination qu'il a collectés.
- 15) Le serveur PrefTreat-AS envoie un message à la fonction d'authentification (PrefTreat-A), qui vérifie si le numéro PIN d'utilisateur fourni est valable.
- 16) La fonction d'authentification valide le numéro PIN par rapport à l'ensemble de services autorisés et indique au serveur PrefTreat-AS si l'utilisateur est un utilisateur valable pour lancer des appels à traitement préférentiel. Une autre possibilité est d'indiquer au serveur PrefTreat-AS quels sont les services autorisés pour cet utilisateur et le serveur PrefTreat-AS détermine si le service demandé est inclus dans cette liste.
- 17) Le serveur PrefTreat-AS envoie un message reINVITE à l'UA appelant.
- 18) Le serveur PrefTreat-AS se déconnecte du serveur PrefTreat-MS avec un message BYE.
- 19) L'UA appelant envoie un message 200 OK au serveur PrefTreat-AS.
- 20) Le serveur PrefTreat-MS envoie un message 200 OK au serveur PrefTreat-AS.
- 21) Le serveur PrefTreat-AS envoie un message INVITE à la passerelle de signalisation du fournisseur pour une signalisation dans le RTPC.
- 22) La passerelle de signalisation envoie un message 200 OK au serveur PrefTreat-AS.
- 23) Le serveur PrefTreat-AS envoie un message reINVITE à l'UA appelant.
- 24) L'UA appelant envoie un message 200 OK au serveur PrefTreat-AS.
- 25) L'appelant et un téléphone RTPC ont maintenant un appel à traitement préférentiel qui est établi et peuvent échanger des informations qui sont converties entre un format de médias RTP et un format analogique numérisé.



J.262(09)\_F01

**Figure 1 – Flux de messages pour l'établissement d'un appel de VoIP à traitement préférentiel avec authentification par numéro PIN**

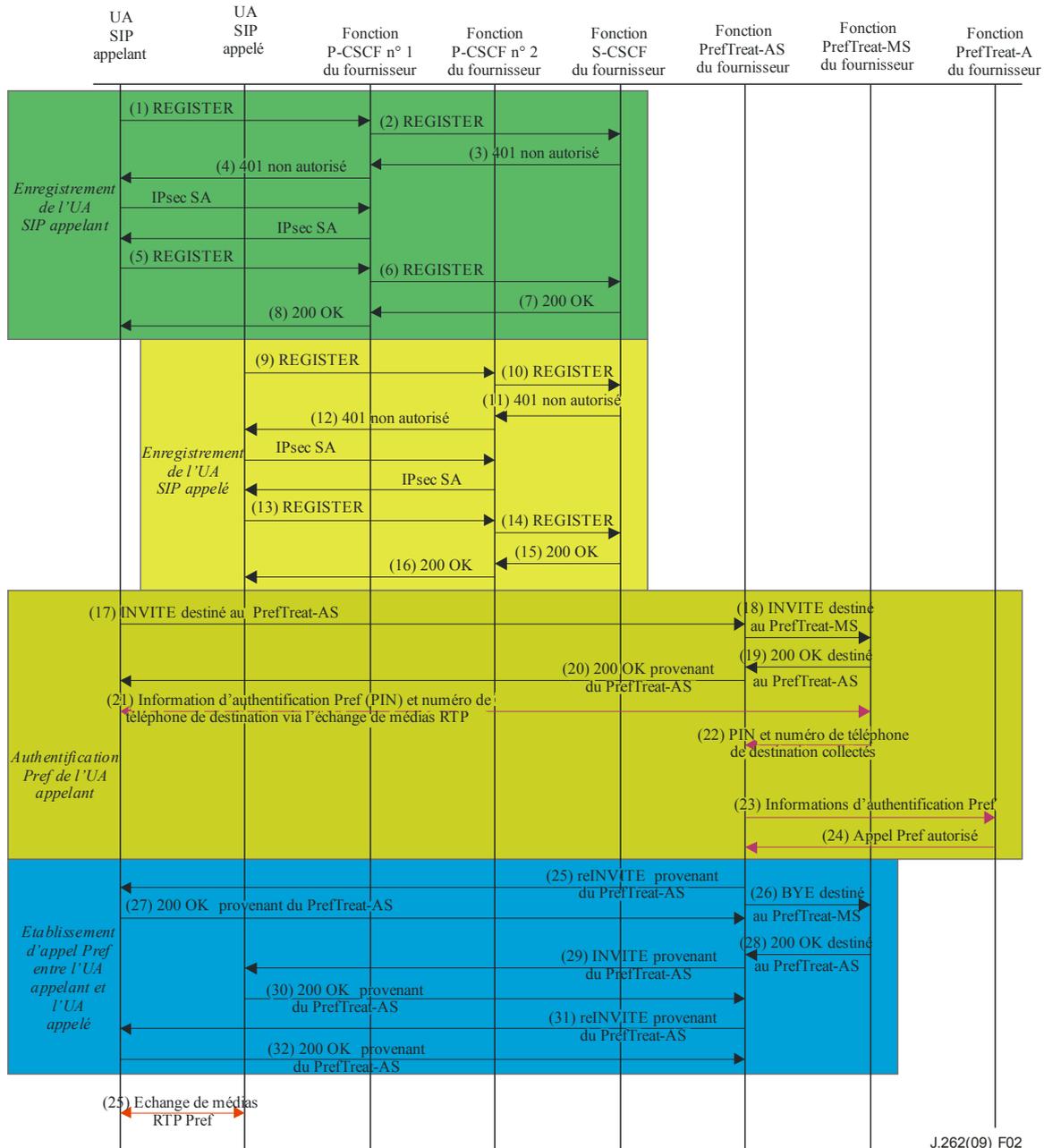
## 6.2 Authentification par numéro PIN dans les réseaux IPCablecom2 – Appel entre deux agents d'utilisateur de VoIP

Les fonctions d'agent d'utilisateur (UA) SIP doivent s'enregistrer auprès de la fonction de traitement d'appel IMS du fournisseur de service de manière à pouvoir lancer et recevoir des appels à signalisation SIP indépendamment du type d'appel. La Figure 2 illustre une demande de traitement préférentiel avec authentification par numéro PIN entre deux UA SIP de VoIP, pour laquelle le demandeur du traitement préférentiel appelle un numéro de téléphone spécial associé à une fonction de serveur d'application pour le traitement préférentiel. Pour l'enregistrement de l'UA appelant et de l'UA appelé et l'authentification par numéro PIN, les étapes de base sont les suivantes (un certain nombre d'accusés de réception et d'autres messages secondaires ne sont pas indiqués). Même si les échanges de messages d'enregistrement ne sont pas propres au traitement préférentiel, ils sont inclus afin de fournir le flux complet:

- 1) L'UA appelant envoie un message REGISTER à la fonction P-CSCF dont il relève, comme au point (1) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 2) La fonction P-CSCF réalise la même activité qu'au point (2) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 3) La fonction S-CSCF crée et envoie une réponse 401 (non autorisé), comme au point (5) de la Figure III.4 de la Recommandation [UIT-T J.360].

- 4) La fonction P-CSCF réalise les mêmes activités concernant la réponse 401 (non autorisé) qu'au point (6) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 5) L'UA appelant réalise les mêmes actions qu'au point (7) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 6) La fonction P-CSCF réalise les mêmes activités concernant le message REGISTER qu'au point (8) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 7) La fonction S-CSCF réalise les mêmes activités et répond par un message 200 OK, comme au point (11) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 8) La fonction P-CSCF retransmet le message 200 OK, comme au point (12) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 9) Comme à l'étape 1) ci-dessus mais entre l'UA appelé et la fonction P-CSCF dont il relève.
- 10) Comme à l'étape 2) ci-dessus mais entre la fonction P-CSCF dont relève l'UA appelé et la fonction S-CSCF.
- 11) Comme à l'étape 3) ci-dessus mais entre la fonction P-CSCF dont relève l'UA appelé et la fonction S-CSCF.
- 12) Comme à l'étape 4) ci-dessus mais entre l'UA appelé et la fonction P-CSCF dont il relève.
- 13) Comme à l'étape 5) ci-dessus mais entre l'UA appelé et la fonction P-CSCF dont il relève.
- 14) Comme à l'étape 6) ci-dessus mais entre la fonction P-CSCF dont relève l'UA appelé et la fonction S-CSCF.
- 15) Comme à l'étape 7) ci-dessus mais entre la fonction P-CSCF dont relève l'UA appelé et la fonction S-CSCF.
- 16) Comme à l'étape 8) ci-dessus mais entre l'UA appelé et la fonction P-CSCF dont il relève.
- 17) L'UA appelant envoie un message INVITE qui est acheminé au serveur d'application PrefTreat-AS, qui est chargé de lancer l'authentification de l'utilisateur.
- 18) Le serveur PrefTreat-AS envoie un message INVITE à un serveur média PrefTreat-MS, qui collectera le numéro PIN de l'utilisateur et les informations relatives à l'UA de destination.
- 19) Le serveur PrefTreat-MS envoie un message 200 OK au serveur PrefTreat-AS.
- 20) Le serveur PrefTreat-AS envoie un message 200 OK à l'UA appelant.
- 21) L'UA appelant et le serveur PrefTreat-MS peuvent maintenant échanger des médias RTP en vue de la collecte du numéro PIN de l'utilisateur et des informations relatives à l'UA de destination saisis par l'utilisateur appelant.
- 22) Le serveur PrefTreat-MS transmet au serveur PrefTreat-AS le numéro PIN de l'utilisateur et les informations relatives à l'UA de destination qu'il a collectés.
- 23) Le serveur PrefTreat-AS envoie un message aux fonctions d'authentification PrefTreat-A, qui vérifient si le numéro PIN d'utilisateur fourni est valable. Une autre possibilité est d'indiquer au serveur PrefTreat-AS quels sont les services autorisés pour cet utilisateur et le serveur PrefTreat-AS détermine si le service demandé est inclus dans cette liste.
- 24) La fonction PrefTreat-A indique au serveur PrefTreat-AS si l'utilisateur est autorisé à lancer le service à traitement préférentiel.
- 25) Le serveur PrefTreat-AS envoie un message reINVITE à l'UA appelant.
- 26) Le serveur PrefTreat-AS se déconnecte du serveur PrefTreat-MS avec un message BYE.
- 27) L'UA appelant envoie un message 200 OK au serveur PrefTreat-AS.
- 28) Le serveur PrefTreat-MS envoie un message 200 OK au serveur PrefTreat-AS.
- 29) Le serveur PrefTreat-AS envoie un message INVITE à l'UA appelé.
- 30) L'UA appelé envoie un message 200 OK au serveur PrefTreat-AS.

- 31) Le serveur PrefTreat-AS envoie un message reINVITE à l'UA appelant.
- 32) L'UA appelant envoie un message 200 OK au serveur PrefTreat-AS.
- 33) Les UA appelant et appelé ont maintenant un appel à traitement préférentiel qui est établi et peuvent échanger des médias RTP.



**Figure 2 – Flux de messages pour le lancement d'un service de VoIP à traitement préférentiel avec authentification par numéro PIN**

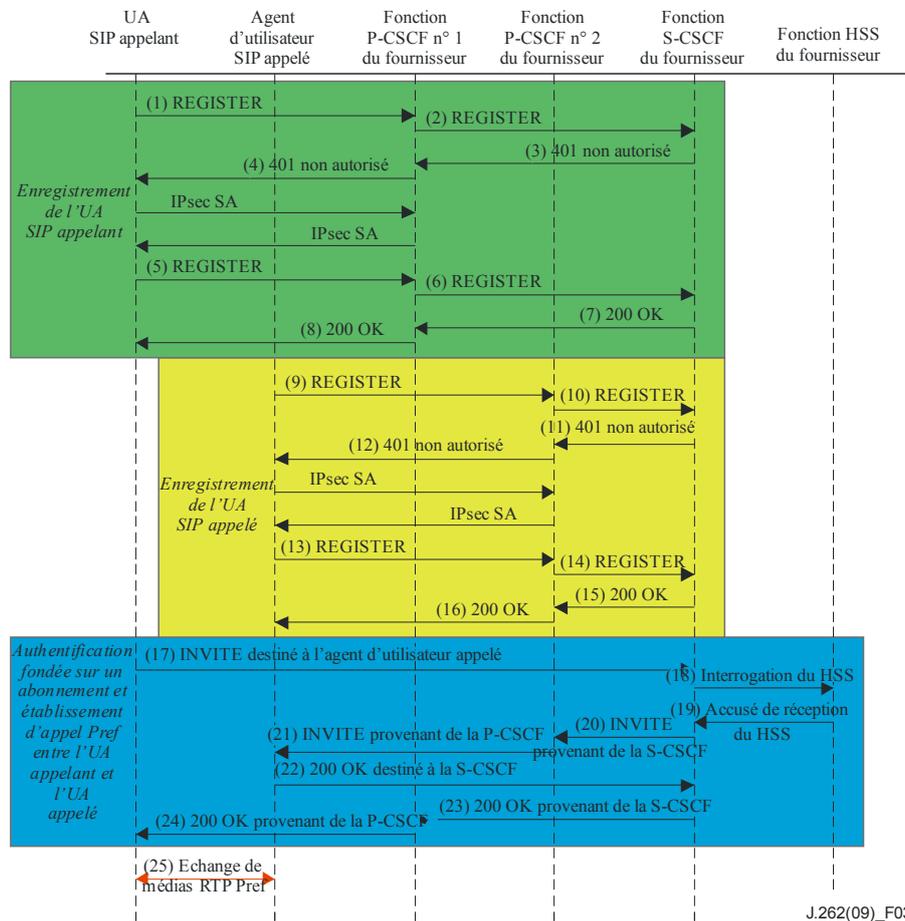
### 6.3 Authentification fondée sur un abonnement aux services à traitement préférentiel dans les réseaux IPCablecom2 – Appels entre deux agents d'utilisateur de VoIP – Priorité signalée par l'agent d'utilisateur au moyen de l'en-tête R-P dans le message INVITE

Les fonctions d'agent d'utilisateur (UA) SIP doivent s'enregistrer auprès de la fonction de traitement d'appel IMS du fournisseur de service de manière à pouvoir lancer et recevoir des appels à signalisation SIP indépendamment du type d'appel. La Figure 3 illustre une demande de traitement préférentiel avec authentification fondée sur un abonnement entre deux UA SIP de VoIP, pour

laquelle le demandeur appelle un numéro de téléphone spécial associé à une fonction de serveur d'application pour le traitement préférentiel. Pour l'enregistrement de l'UA appelant et de l'UA appelé et l'authentification fondée sur un abonnement pour le traitement préférentiel, les étapes de base sont les suivantes (un certain nombre d'accusés de réception et d'autres messages secondaires ne sont pas indiqués). Même si les échanges de messages d'enregistrement ne sont pas propres au traitement préférentiel, ils sont inclus afin de fournir le flux complet:

- 1) L'UA appelant envoie un message REGISTER à la fonction P-CSCF dont il relève, comme au point (1) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 2) La fonction P-CSCF réalise la même activité qu'au point (2) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 3) La fonction S-CSCF crée et envoie une réponse 401 (non autorisé), comme au point (5) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 4) La fonction P-CSCF réalise les mêmes activités concernant la réponse 401 (non autorisé) qu'au point (6) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 5) L'UA appelant réalise les mêmes actions qu'au point (7) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 6) La fonction P-CSCF réalise les mêmes activités concernant le message REGISTER qu'au point (8) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 7) La fonction S-CSCF réalise les mêmes activités et répond par un message 200 OK, comme au point (11) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 8) La fonction P-CSCF retransmet le message 200 OK, comme au point (12) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 9) Comme à l'étape 1) ci-dessus mais entre l'UA appelé et la fonction P-CSCF dont il relève.
- 10) Comme à l'étape 2) ci-dessus mais entre la fonction P-CSCF dont relève l'UA appelé et la fonction S-CSCF.
- 11) Comme à l'étape 3) ci-dessus mais entre la fonction P-CSCF dont relève l'UA appelé et la fonction S-CSCF.
- 12) Comme à l'étape 4) ci-dessus mais entre l'UA appelé et la fonction P-CSCF dont il relève.
- 13) Comme à l'étape point 5) ci-dessus mais entre l'UA appelé et la fonction P-CSCF dont il relève.
- 14) Comme à l'étape 6) ci-dessus mais entre la fonction P-CSCF dont relève l'UA appelé et la fonction S-CSCF.
- 15) Comme à l'étape 7) ci-dessus mais entre la fonction P-CSCF dont relève l'UA appelé et la fonction S-CSCF.
- 16) Comme à l'étape 8) ci-dessus mais entre l'UA appelé et la fonction P-CSCF dont il relève.
- 17) L'UA appelant envoie un message INVITE qui est acheminé à la fonction S-CSCF. Le message INVITE inclut un en-tête R-P indiquant un traitement prioritaire.
- 18) La fonction S-CSCF interroge le serveur HSS pour déterminer si entre l'UA appelant est autorisé à lancer un appel de service à traitement préférentiel.
- 19) Le serveur HSS répond à la fonction S-CSCF, soit par une autorisation (accusé de réception), soit par un refus d'autorisation.
- 20) La fonction S-CSCF envoie un message INVITE à la fonction P-CSCF dont relève l'UA appelé.
- 21) La fonction P-CSCF dont relève l'UA appelé retransmet le message INVITE à l'UA appelé.
- 22) L'UA appelé envoie un message 200 OK à la fonction S-CSCF.

- 23) La fonction S-CSCF envoie un message 200 OK à la fonction P-CSCF dont relève l'UA appelant.
- 24) La fonction P-CSCF dont relève l'agent d'utilisateur appelant envoie un message 200 OK à l'UA appelant.
- 25) Les UA appelant et appelé ont maintenant un appel à traitement préférentiel qui est établi et peuvent échanger des médias RTP.



**Figure 3 – Flux de messages pour une authentification fondée sur un abonnement VoIP – Priorité signalée par l'agent d'utilisateur au moyen de l'en-tête R-P dans le message INVITE**

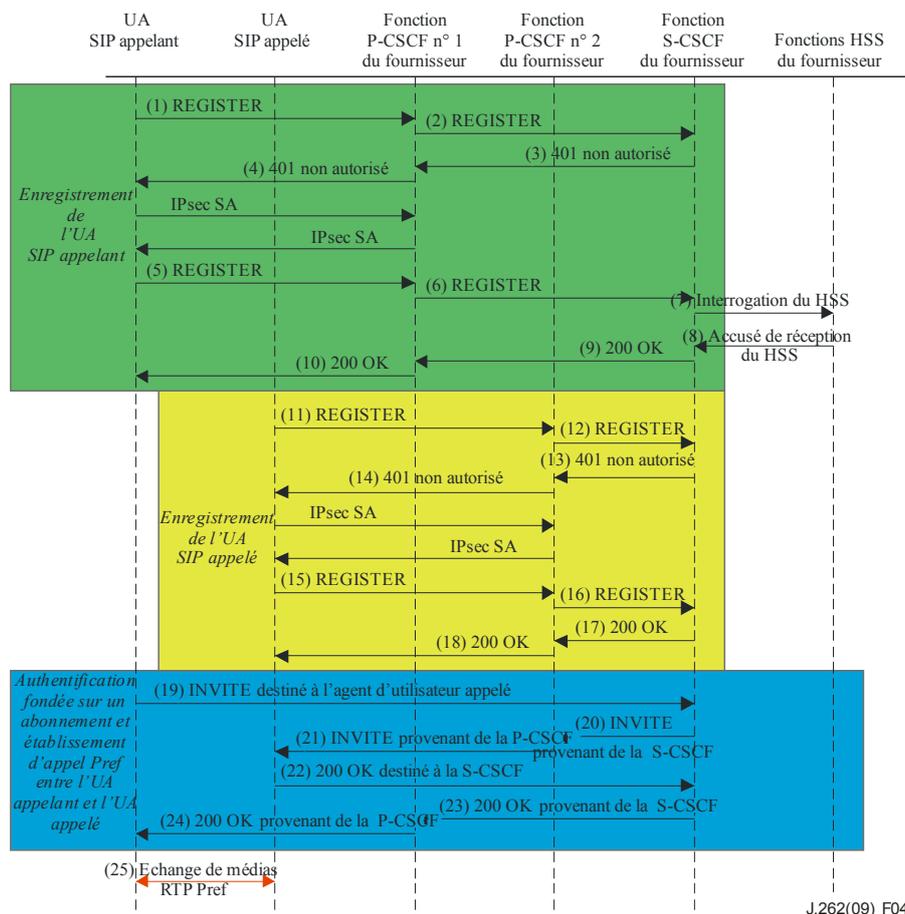
#### 6.4 Authentification fondée sur un abonnement aux services à traitement préférentiel dans les réseaux IPCablecom2 – Appels entre deux agents d'utilisateur de VoIP – Priorité signalée par l'agent d'utilisateur au moyen d'un identificateur

La Recommandation [b-UIT-T J.263] définit deux options pour indiquer qu'un appel doit bénéficier d'un traitement préférentiel. Dans le présent paragraphe, l'agent d'utilisateur (UA) envoie un identificateur qui est inclus comme déclencheur dans les critères de filtrage initial contenus dans le profil d'utilisateur. Le flux d'appel est le même que sur la Figure 3 sauf pour les étapes suivantes. C'est après l'étape 6, à laquelle la fonction P-CSCF envoie un message REGISTER à la fonction S-CSCF, qu'une demande est envoyée au serveur HSS pour obtenir le profil d'utilisateur et non après la réception du message INVITE à l'étape 18. Le serveur HSS retourne les critères de filtrage initial pour l'utilisateur, qui permettent notamment de détecter des identificateurs (par exemple un code de fonctionnalité avec un numéro spécial de destination ou un numéro spécial d'accès avec un numéro PIN sont définis) afin de déterminer que l'utilisateur demande un appel à traitement préférentiel. Les étapes 18 et 19 ont lieu pendant l'enregistrement et non après l'envoi du message INVITE à l'étape 17. On utilise les critères de filtrage initial pour déterminer le serveur

d'application pour le traitement préférentiel auquel la demande INVITE est retransmise. A l'étape 17, le message INVITE inclut l'identificateur dans l'en-tête SDP et non dans l'en-tête R-P comme dans le cas précédent. L'identificateur déclenche le traitement préférentiel au niveau de la fonction P-CSCF au niveau de laquelle l'en-tête R-P est inséré avec la valeur de priorité appropriée indiquée dans la Recommandation [b-UIT-T J.263].

- 1) L'UA appelant envoie un message REGISTER à la fonction P-CSCF dont il relève, comme au point (1) de la Figure III.4 de la Recommandation [UIT-T J.360]. Ce message contient un identificateur indiquant un utilisateur de service de télécommunication à traitement préférentiel.
- 2) La fonction P-CSCF réalise la même activité qu'au point (2) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 3) La fonction S-CSCF crée et envoie une réponse 401 (non autorisé), comme au point (5) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 4) La fonction P-CSCF réalise les mêmes activités concernant la réponse 401 (non autorisé) qu'au point (6) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 5) L'UA appelant réalise les mêmes actions qu'au point (7) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 6) La fonction P-CSCF réalise les mêmes activités concernant le message REGISTER qu'au point (8) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 7) La fonction S-CSCF interroge le serveur HSS pour déterminer si l'UA appelant est autorisé à lancer un appel de service à traitement préférentiel.
- 8) En cas d'autorisation, le serveur HSS retourne les critères de filtrage initial pour l'utilisateur, qui permettent notamment de détecter des identificateurs (par exemple un code de fonctionnalité avec un numéro spécial de destination ou un numéro spécial d'accès avec un numéro PIN sont définis) afin de déterminer que l'utilisateur demande un appel à traitement préférentiel. Dans le cas contraire, il retourne "non autorisé".
- 9) La fonction S-CSCF répond par un message 200 OK, comme au point (11) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 10) La fonction P-CSCF retransmet le message 200 OK, comme au point (12) de la Figure III.4 de la Recommandation [UIT-T J.360].
- 11) Comme à l'étape 1) ci-dessus mais entre l'UA appelé et la fonction P-CSCF dont il relève.
- 12) Comme à l'étape 2) ci-dessus mais entre la fonction P-CSCF dont relève l'UA appelé et la fonction S-CSCF.
- 13) Comme à l'étape 3) ci-dessus mais entre la fonction P-CSCF dont relève l'UA appelé et la fonction S-CSCF.
- 14) Comme à l'étape 4) ci-dessus mais entre l'UA appelé et la fonction P-CSCF dont il relève.
- 15) Comme au point 5) ci-dessus mais entre l'UA appelé et la fonction P-CSCF dont il relève.
- 16) Comme à l'étape 6) ci-dessus mais entre la fonction P-CSCF dont relève l'UA appelé et la fonction S-CSCF.
- 17) Comme à l'étape 9) ci-dessus mais entre la fonction P-CSCF dont relève l'UA appelé et la fonction S-CSCF.
- 18) Comme à l'étape 10) ci-dessus mais entre l'UA appelé et la fonction P-CSCF dont il relève.
- 19) L'UA appelant envoie un message INVITE avec l'identificateur d'utilisateur préférentiel qui est acheminé à la fonction S-CSCF.
- 20) La fonction S-CSCF envoie un message INVITE à la fonction P-CSCF dont relève l'UA appelé.

- 21) La fonction P-CSCF dont relève l'agent d'utilisateur appelé retransmet le message INVITE à l'UA appelé.
- 22) L'UA appelé envoie un message 200 OK à la fonction S-CSCF.
- 23) La fonction S-CSCF envoie un message 200 OK à la fonction P-CSCF dont relève l'UA appelant.
- 24) La fonction P-CSCF dont relève l'UA appelant envoie un message 200 OK à l'UA appelant.
- 25) Les UA appelant et appelés ont maintenant un appel à traitement préférentiel qui est établi et peuvent échanger des médias RTP.



**Figure 4 – Flux de messages pour une authentification basée sur un abonnement VoIP – Priorité signalée par l'agent d'utilisateur au moyen d'un identificateur**

## 7 Prescriptions d'authentification pour les services de télécommunication à traitement préférentiel dans les réseaux IPCablecom2

On trouvera ci-après des prescriptions spécifiques d'authentification pour les sessions de télécommunication à traitement préférentiel dans l'architecture IPCablecom2.

En cas d'utilisation dans les équipements d'utilisateur, ceux-ci doivent pouvoir stocker en toute sécurité les noms d'utilisateur et les mots de passe de manière à réduire le plus possibles les risques. Si cette approche est utilisée, l'équipement d'utilisateur doit inviter les utilisateurs à saisir leur nom d'utilisateur et leur mot de passe.

## Bibliographie

- [b-UIT-T E.106] Recommandation UIT-T E.106 (2003), *Plan international de priorité en période de crise destiné aux opérations de secours en cas de catastrophe (IEPS)*.
- [b-UIT-T J.263] Recommandation UIT-T J.263 (2009), *Spécifications relatives à la priorité pour les télécommunications à traitement préférentiel sur les réseaux IPCablecom2*.
- [b-UIT-T J.366.8] Recommandation UIT-T J.366.8 (2006), *Sous-système multimédia IP du système IPCablecom2 (IMS): Spécification de la sécurité d'un domaine de réseau*.
- [b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.
- [b-UIT-T Y.1271] Recommandation UIT-T Y.1271 (2004), *Cadres généraux applicables aux spécifications et aux capacités de réseau pour la prise en charge des télécommunications d'urgence sur les réseaux à commutation de circuits et à commutation de paquets en cours d'évolution*.
- [b-UIT-T Y.2205] Recommandation UIT-T Y.2205 (2008), *Réseaux de prochaine génération – Télécommunications d'urgence – Considérations techniques*.
- [b-UIT-T Y.2702] Recommandation UIT-T Y.2702 (2008), *Spécifications d'authentification et d'autorisation pour les réseaux de prochaine génération version 1*.
- [b-IETF RFC 2560] IETF RFC 2560 (1999), *X509 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*.





## SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
<b>Série J</b>	<b>Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias</b>
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication