Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1256

(03/2016)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberespace – Gestion des identités

Lignes directrices et cadre pour le partage des résultats d'authentification réseau avec des applications de services

Recommandation UIT-T X.1256

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	**X.1250–X.1279**
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
Recommandations relatives aux infrastructures de clé publique	X.1340–X.1349
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1256

Lignes directrices et cadre pour le partage des résultats d'authentification réseau avec des applications de services

Résumé

Du fait de la multiplication rapide des dispositifs mobiles et des applications connectés à l'Internet, l'environnement des services et du réseau est de plus en plus complexe. Il est donc urgent de simplifier le mécanisme d'authentification de l'utilisateur, afin d'améliorer l'expérience de ce dernier ainsi que la qualité de service.

De nombreuses organisations de normalisation, parmi lesquelles l'UIT-T, ont accompli un important travail de recherche sur le mécanisme d'authentification unifié. Cependant, les travaux actuels se concentrent tous, en substance, sur l'authentification unifiée parmi plusieurs applications de services, sans tenir compte des liens avec l'authentification réseau.

Du point de vue de l'opérateur de réseau, l'utilisateur se soumet à certaines formes d'authentification lorsqu'il se connecte. Mais cette première «authentification réseau» n'est pas réutilisée lorsqu'il s'identifie à nouveau pour accéder à un service. La mise en place d'un mécanisme de partage des résultats d'authentification permet aux applications du service d'identifier un utilisateur grâce aux résultats d'authentification fournis par le réseau. Ainsi, l'utilisateur ne s'identifie qu'une seule fois, par le biais du réseau, et peut ensuite accéder directement au service souhaité.

La présente Recommandation UIT-T X.1256 expose des lignes directrices à l'intention des opérateurs de réseau et des fournisseurs de services en vue du partage des résultats d'authentification réseau, et offre un cadre général pour le partage d'un nombre minimal d'attributs entre de multiples services, le tout dans une relation de confiance solide.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1256	23-03-2016	17	11.1002/1000/12605

Mots clés

Authentification, attributs d'identité, authentification de niveau réseau

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

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/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1256

Lignes directrices et cadre pour le partage des résultats d'authentification réseau avec des applications de service

1 Domaine d'application

La présente Recommandation décrit des lignes directrices à l'intention des opérateurs de réseau et des fournisseurs de services pour le partage des résultats d'authentification réseau, et offre un cadre général pour le partage d'un nombre minimal d'attributs entre de multiples services, le tout dans une relation de confiance solide.

Les méthodes appliquées par les opérateurs de réseau pour effectuer, intégrer ou mettre au point une authentification de niveau réseau n'entrent pas dans le champ de la présente Recommandation.

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 d'une Recommandation.

[UIT-T X.1254] Recommandation UIT-T X.1254 (2012), *Cadre de garantie d'authentification des entités*.

3 Définitions

3.1 Termes définis ailleurs

Aucun.

3.2 Termes définis dans la présente Recommandation

Aucun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

2G/3G deuxième/troisième génération

AC unité de contrôle d'accès (*access controller*)

AKA authentification et concordance de clés (*authentication and key agreement*)

AN réseau d'accès (*access network*)

AP point d'accès (*access point*)

API interface de programmation d'applications (*application programming interface*)

AUG passerelle d'authentification (*authentication gateway*)

BRAS serveur d'accès distant à large bande (*broadband remote access server*)

EAP-SIM méthode de protocole d'authentification extensible pour les modules d'identité des abonnées (GSM) (*extensible authentication protocol method for (GSM) subscriber identity modules*)

GGSN noeud de support GPRS de passerelle (*gateway GPRS support node*)

GPRS Service général de radiocommunication en mode paquet (*general packet radio service*)

HTTP protocole de transfert hypertexte (*hyper text transfer protocol*)

IMPI identité privée multimédia IP (*IP multimedia private identity*)

IMPU identité d'utilisateur public multimédia IP (*IP multimedia public user identity*)

IMS sous-système multimédia IP (*IP multimedia subsystem*)

IMSI identité internationale d'abonné mobile (*international mobile subscriber identity*)

IP protocole Internet (*internet protocol*)

LoA Niveau de garantie (*level of assurance*)

MSISDN numéro RNIS/RTPC international d'abonné mobile (*mobile subscriber international ISDN/PSTN number*)

RADIUS service d'authentification à distance des utilisateurs entrants (*remote authentication dial-in user service*)

RNIS réseau numérique à intégration de services

RTPC réseau téléphonique public commuté

SGSN noeud de support GPRS de service (*serving GPRS support node*)

SIM module d'identification de l'abonné (*subscriber identity module*)

SIP protocole d'ouverture de session (*session initiation protocol*)

SNS service de réseau social (*social network service*)

UE équipement d'utilisateur (*user equipment*)

USIM module d'identité d'abonné universel (*universal subscriber identity module*)

URI identificateur uniforme de ressource (*uniform resource identifier*)

WAP protocole d'application sans fil (*wireless application protocol*)

WLAN réseau local hertzien (*wireless local area network*)

5 Conventions

Aucune.

6 Mécanismes de partage d'attributs d'authentification

6.1 Cadre général

Lorsque des utilisateurs accèdent à un réseau d'opérateur, le réseau d'accès doit les identifier avec un degré de fiabilité élevé. Mais pour les services, cette authentification est souvent une source de complexité. Dans la plupart des cas, les utilisateurs finals sont authentifiés deux fois: sur le réseau, puis dans le système de fourniture de services. Par exemple, l'utilisateur est authentifié par le réseau de troisième génération (3G) au moyen de la carte de module d'identité d'abonné universel (USIM) de son téléphone cellulaire (matériel en sa possession), puis lorsqu'il se connecte à un service de réseau social (service SNS), il fait l'objet d'une deuxième authentification, cette fois par le serveur

web, sur la base d'un identifiant et d'un mot de passe enregistrés préalablement (informations connues de l'utilisateur).

Le principe fondamental du partage d'attributs d'authentification est de permettre aux différents services d'utiliser les attributs d'authentification réseau. Le cadre général de ce principe est présenté à la Figure 6-1.

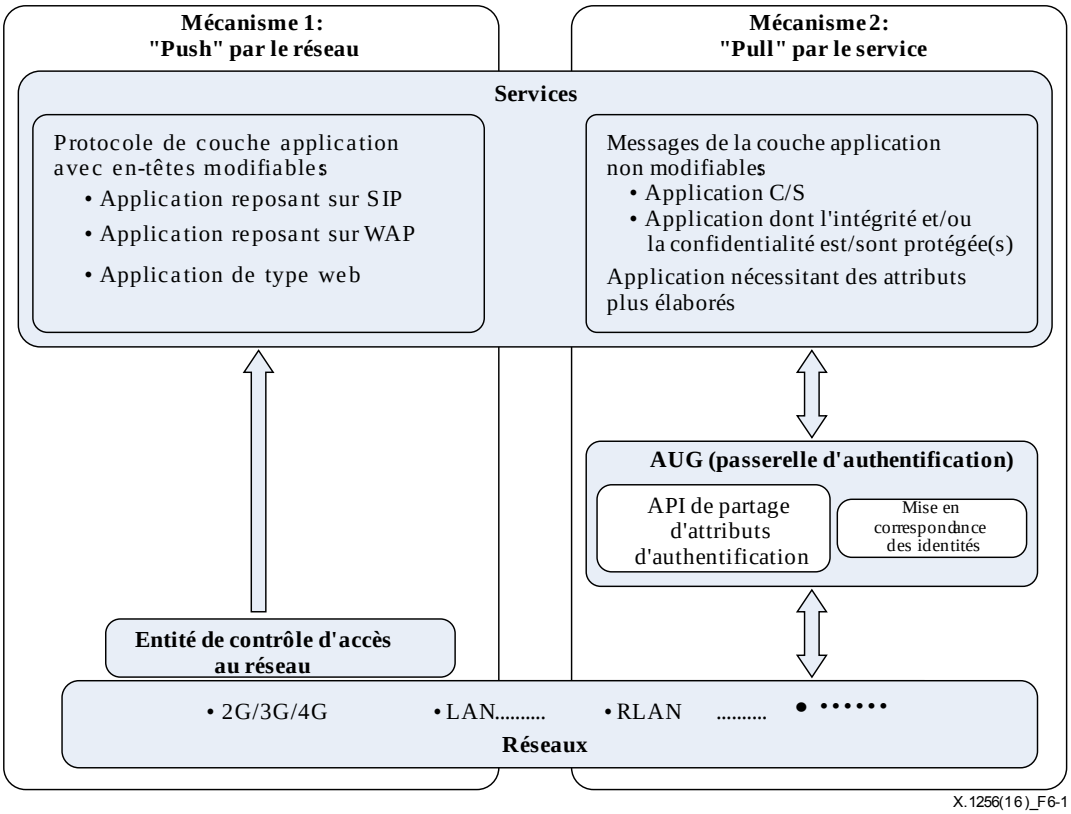

Figure 6-1 – Cadre général du partage d'attributs d'authentification réseau avec les applications de service

Ce cadre général comporte deux types de mécanismes de partage d'attributs d'authentification:

- Mécanisme 1 – Mécanisme de «push» par le réseau: transfert direct des attributs d'authentification réseau vers les applications de service

  Lorsque l'entité de contrôle d'accès au réseau est en mesure de comprendre le protocole de couche application du service (SIP, WAP, HTTP, etc.), elle peut insérer les attributs d'authentification réseau dans les messages de la couche application et les transférer directement vers la plate-forme de services. Dans ce cas, il est inutile de définir une interface de programmation d'applications (API) permettant aux applications de service de demander expressément les attributs d'authentification. En effet, elles les reçoivent automatiquement via les en-têtes de message.

  De deux choses l'une: soit les applications de service décident d'analyser et d'utiliser les en-têtes insérés par le réseau, soit elles les ignorent. Les applications de service qui ont besoin d'autres attributs que ceux «poussés» par le réseau doivent les «tirer» en utilisant le mécanisme de «pull» du service.

  Voir l'Appendice I.1 qui décrit un cas d'utilisation concret.

- Mécanisme 2 – Mécanisme de «pull» par le service: les attributs d'authentification réseau sont partagés via la passerelle d'authentification (AUG).

  Si l'entité de contrôle d'accès au réseau ne peut pas analyser ou modifier les messages de couche application du service (par exemple, lorsque le protocole de couche application est

propre à un constructeur ou que l'intégrité et/ou la confidentialité des messages de couche application sont protégées), il est nécessaire de mettre en place, dans le réseau, une passerelle AUG autonome, dont le rôle est de partager les attributs d'authentification. Cette passerelle met en oeuvre des API de réseau clairement spécifiées, que les applications de service peuvent invoquer pour obtenir, de la part du réseau, les attributs d'authentification requis.

De plus, lorsque les applications de service mentionnées ci-dessus dans le mécanisme de «push» ont besoin d'autres attributs que ceux transmis par le réseau, elles doivent aussi utiliser le mécanisme de «pull» par le service.

Voir l'Appendice I.2 qui décrit un cas d'utilisation concret.

6.2 Mécanisme de «push» par le réseau

6.2.1 Guide de mise en oeuvre

Lorsqu'un utilisateur se connecte au réseau, son identité est authentifiée par l'entité de contrôle d'accès située à l'interface du réseau. Parmi les exemples types d'entités de contrôle d'accès au réseau, citons l'unité de contrôle d'accès (AC) du réseau local hertzien (WLAN), le noeud de support GPRS de service (SGSN) ou le noeud de support GPRS de passerelle (GGSN) d'un réseau de service général de radiocommunication en mode paquet (GPRS) ou encore le serveur d'accès distant à large bande (BRAS) d'un réseau fixe. Une fois l'authentification réseau réalisée, l'entité de contrôle d'accès au réseau connaît l'identité de l'utilisateur.

Lorsque l'entité de contrôle d'accès au réseau est en mesure de comprendre le protocole de couche application du service (SIP, WAP, HTTP, etc.), elle peut encapsuler l'identité de l'utilisateur ainsi que d'autres données connexes dans les messages de requête du service et transmettre ces informations à la plate-forme de services.

Si la plate-forme de services juge que l'entité de contrôle d'accès au réseau est fiable, elle peut extraire directement l'identité de l'utilisateur en analysant les requêtes de service et considérer que l'utilisateur est déjà authentifié.

Dans cette architecture, la plate-forme de services a besoin de déterminer si elle peut ou non se fier aux attributs d'authentification insérés par l'entité de contrôle d'accès au réseau. Pour cela, l'opérateur du réseau doit passer un contrat avec le fournisseur de services et lui transmettre une liste des entités de contrôle d'accès fiables ou lui fournir un mécanisme permettant de vérifier l'identité de ces entités (clés prépartagées, certificats numériques, etc.). Les informations d'utilisateur transmises entre l'entité de contrôle d'accès et la plate-forme de services doivent être protégées. Les entités de contrôle d'accès au réseau doivent tenir à jour une «liste blanche» des plates-formes de services ayant passé le contrat en question, et les attributs d'authentification réseau ne doivent être transmis qu'aux plates-formes de services figurant sur cette liste. Les lignes directrices à suivre pour établir cette relation de confiance sortent du cadre de la présente Recommandation.

6.2.2 Description de l'interface

Les attributs d'authentification réseau sont insérés dans la partie de l'en-tête des messages de requête de service réservée au protocole d'application (SIP, HTTP, etc.) et transférés de l'entité de contrôle d'accès au réseau vers la plate-forme de services.

Les attributs suivants doivent être transmis:

1) Identité de l'utilisateur:

   Ce champ contient l'identité réseau de l'utilisateur (identificateur URI du protocole SIP, numéro MSISDN, nom d'utilisateur, etc.). La plate-forme de services peut utiliser ce champ pour identifier l'utilisateur.

2) Méthode d'authentification avec niveau de garantie (LoA) connu [UIT-T X.1254]:

Ce champ contient l'identifiant de la méthode d'authentification (2G/3G/4G AKA, IMS AKA, HTTP/SIP Digest, EAP-SIM, etc.).

L'opérateur de réseau et les fournisseurs de services doivent convenir de la liste des identifiants et des niveaux LoA des méthodes d'authentification reconnaissables.

Chaque plate-forme de services doit décider, à partir du niveau LoA de la méthode d'authentification et de sa propre politique de sécurité, si elle accepte ou non les attributs d'authentification transmis par le réseau (méthode).

3) Autres attributs figurant dans le contrat passé entre l'opérateur et le fournisseur de services.

6.3 Mécanisme de «pull» par le service

6.3.1 Guide de mise en oeuvre

Il est impossible de mettre en oeuvre le mécanisme de «push» par le réseau lorsque l'entité de contrôle d'accès au réseau ne peut pas analyser ou modifier les messages de couche application du service (par exemple, lorsque le protocole de couche application est propre à un constructeur, ou que les messages de service sont chiffrés ou que leur intégrité est protégée). Dans ce cas, une solution consiste à placer, entre le réseau et la plate-forme de services, une passerelle AUG qui, jouant le rôle de serveur proxy pour la plate-forme, lui fournit les attributs d'authentification réseau.

Il est aussi justifié de recourir au modèle de «pull» par le service lorsque les attributs intégrés aux messages poussés par le réseau ne sont pas adaptés à une requête de service particulière. En pareil cas, la plate-forme de services peut avoir besoin d'interroger le réseau pour obtenir des informations complémentaires sur les attributs d'authentification réseau.

Pour mettre en oeuvre le modèle de «pull» par le service, la passerelle AUG doit exporter un ensemble d'API réseau, que les applications de service peuvent invoquer pour obtenir, de la part du réseau, diverses informations sur les résultats de l'authentification. Comme le réseau et les plates-formes de services utilisent éventuellement des identifiants d'utilisateur différents, la passerelle AUG doit comporter une fonction de mise en correspondance des identifiants permettant de relier l'identifiant de service d'un utilisateur à son identifiant réseau, et inversement.

Dans cette architecture, il est nécessaire que la plate-forme de services et la passerelle AUG se fassent mutuellement confiance. Pour cela, l'opérateur du réseau doit passer un contrat avec le fournisseur de services et lui transmettre soit une liste des passerelles AUG fiables, soit un mécanisme permettant d'identifier ces passerelles (clés prépartagées, certificats numériques, etc.). Les informations d'utilisateur transmises entre la passerelle AUG et la plate-forme de services doivent être protégées. De leur côté, les passerelles AUG doivent appliquer aux API exportées un mécanisme d'autorisation («liste blanche» par exemple) pour que les attributs d'authentification réseau ne puissent être communiqués qu'aux plates-formes de services ayant passé le contrat. Les lignes directrices à suivre pour établir cette relation de confiance sortent du cadre de la présente Recommandation.

6.3.2 Description de l'interface

La passerelle AUG met en oeuvre des API de réseau clairement spécifiées, que les applications de service peuvent invoquer pour obtenir, de la part du réseau, les attributs d'authentification.

Les opérateurs de réseau sont libres de concevoir les API sous la forme qui leur convient. La procédure à suivre pour établir cette relation de confiance sort du cadre de la présente Recommandation.

Tout type d'information lié aux utilisateurs authentifiés du réseau est susceptible d'être transmis via ces API: emplacement de l'utilisateur, informations concernant son inscription, ses statistiques d'utilisation réseau, etc.

7 Considérations touchant à la sécurité

Lors de la mise en place de solutions techniques relevant du cadre général décrit au paragraphe 6, il convient de noter certains points liés à la sécurité:

- Il est indispensable de protéger les éléments d'authentification sur le réseau et de garantir la fiabilité et la sécurité des capacités d'authentification du réseau.
- Pour s'assurer de la fiabilité des attributs d'authentification transmis par le réseau, les systèmes de service doivent établir une relation de confiance avec ce dernier. Pour prévenir le risque d'usurpation de l'identité du serveur d'authentification, les plates-formes de service ne doivent se fier qu'aux informations d'identité d'utilisateur provenant de serveurs d'authentification connus.
- Il est de la plus haute importance que les attributs d'authentification soient transmis à la plate-forme de service de manière sécurisée. La confidentialité et l'intégrité des informations d'identité des utilisateurs doivent être garanties; leur transmission doit être protégée contre les attaques par rejet et par falsification.
- Lorsqu'il transmet à la plate-forme de services des résultats d'authentification et d'autres informations concernant l'utilisateur, le réseau doit se conformer strictement aux législations et aux textes réglementaires applicables en matière de protection de la vie privée dans la juridiction où le service est fourni.
- La plate-forme de services doit gérer de façon appropriée les informations d'authentification d'utilisateur reçues du réseau; elle doit notamment les mémoriser en toute sécurité en vue d'une utilisation future et les détruire rapidement après utilisation. Il convient de prévenir l'utilisation abusive et la perte des données d'utilisateur.

Appendice I

Cas d'utilisation

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

I.1 Méthode de «push» par le réseau: cas d'utilisation

I.1.1 Réseau 2G/3G/4G vers service WAP

Le protocole d'application sans fil WAP est un service de données mobile qui connaît un certain succès. Il est accessible via les réseaux 2G/3G/4G. Après rattachement au réseau et authentification, la passerelle WAP (ou «WAP GW», *WAP gateway*) insère le numéro RNIS/RTPC international d'abonné mobile (MSISDN) de l'utilisateur dans les requêtes WAP entrantes. Le serveur WAP extrait le numéro MSISDN de la requête et identifie l'utilisateur directement à partir de ce numéro ou indirectement par mise en correspondance du numéro avec un identifiant d'utilisateur enregistré.

La réservation des taxis est un exemple type d'application basée sur le service WAP. A partir de son téléphone cellulaire, l'utilisateur peut visiter un site WAP offrant ce service sans fournir son véritable nom. Pour l'identifier et traiter sa ou ses demandes, le serveur WAP utilise le numéro MSISDN. Si le chauffeur de taxi a besoin de contacter l'utilisateur, il lui suffit de rappeler ce numéro.

Le serveur WAP peut en outre exiger l'enregistrement préalable de l'utilisateur, qui se voit attribuer un identifiant associé à un ou plusieurs numéros MSISDN. Dans ce cas, avant de traiter la demande, le serveur WAP a besoin de mettre en correspondance le numéro MSISDN poussé par le réseau et un identifiant d'utilisateur enregistré.

La procédure technique détaillée est exposée ci-dessous (Figure I.1):

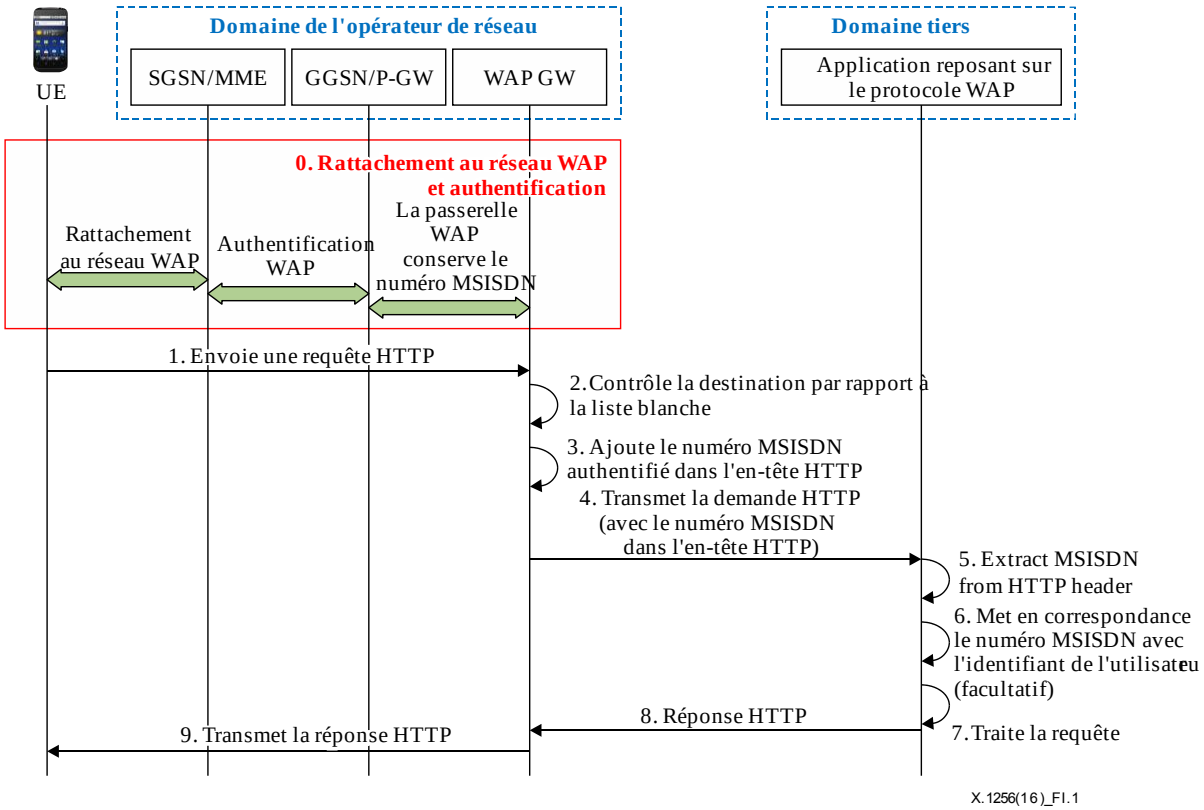

Figure I.1 – Partage d'authentification avec un service WAP via un réseau 2G/3G/4G

0 L'équipement d'utilisateur UE se rattache au réseau 2G/3G/4G. La passerelle WAP conserve le numéro MSISDN de chaque utilisateur authentifié.

1 L'équipement d'utilisateur envoie une requête en utilisant le protocole de transfert hypertexte (HTTP) pour accéder à un service WAP.

2 La passerelle WAP (WAP GW) reçoit la requête et vérifie si la destination offrant le service est sur la liste blanche.

3 Si l'adresse de la destination est sur la liste blanche, la passerelle WAP insère un nouveau champ dans l'en-tête HTTP de la requête (par exemple, «x-up-calling-line-id»); ce champ contient le numéro MSISDN de l'utilisateur.

4 La passerelle WAP transmet la requête HTTP modifiée au serveur WAP.

5 Le serveur WAP extrait de l'en-tête HTTP le numéro MSISDN de l'utilisateur.

6 A titre facultatif, le serveur WAP met en correspondance le numéro MSISDN et un identifiant d'utilisateur enregistré.

7 Le serveur WAP traite la requête en fonction du numéro MSISDN ou de l'identifiant de l'utilisateur correspondant à ce numéro.

8 Le serveur WAP envoie la réponse HTTP à la passerelle WAP.

9 La passerelle WAP transmet la réponse HTTP à l'équipement d'utilisateur.

I.2 Méthode de «pull» par le service: cas d'utilisation

I.2.1 Service Internet utilisant les attributs de localisation d'un réseau 2G/3G/4G

De nombreux services Internet et Internet mobile reposent sur la géolocalisation. Citons, à titre d'exemple, le cas d'un utilisateur qui se connecte à un service WAP à partir de son téléphone cellulaire pour trouver une banque, un hôtel, un restaurant ou un centre commercial près de l'endroit où il se trouve. Si le téléphone est équipé de la fonction GPS, il peut envoyer les paramètres de géolocalisation de l'utilisateur au serveur WAP dans la requête de recherche. S'il n'est pas compatible GPS ou que cette fonction est momentanément indisponible (intérieur d'un bâtiment par exemple), le serveur WAP peut éventuellement s'appuyer sur le coeur de réseau 2G/3G/4G pour localiser l'utilisateur.

La procédure technique détaillée d'un service Internet exploitant les résultats de la géolocalisation effectuée par un réseau 2G/3G/4G est exposée ci-dessous (Figure I.2):

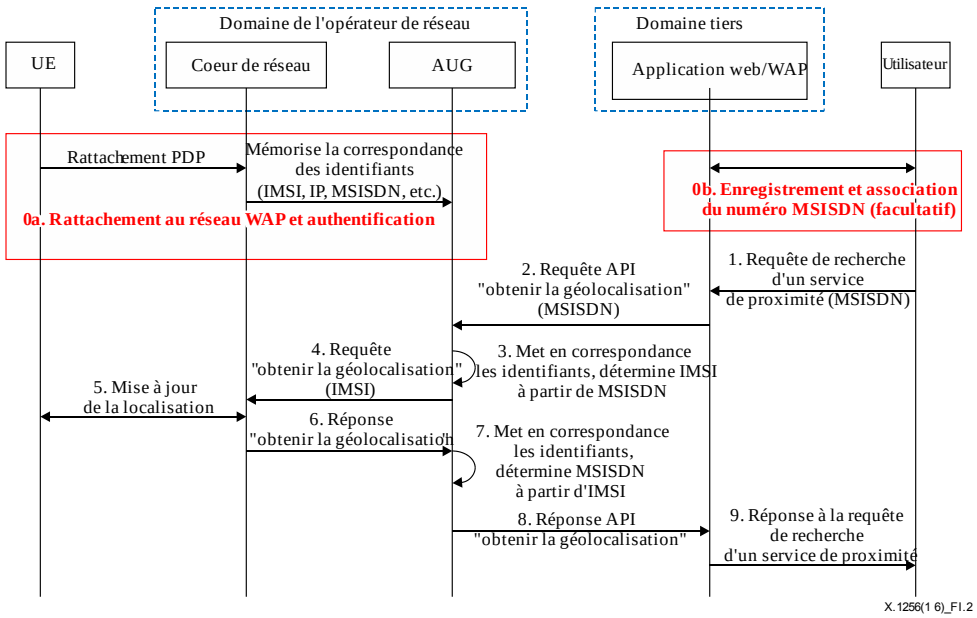

Figure I.2 – Service Internet utilisant les attributs de localisation d'un réseau 2G/3G/4G

0a L'équipement UE se rattache au réseau 2G/3G/4G. La passerelle GGSN/P-GW envoie à la passerelle AUG la relation de correspondance entre l'identité internationale d'abonné mobile

(IMSI), le numéro MSISDN et l'adresse IP de l'utilisateur, au moyen du protocole de service d'authentification à distance des utilisateurs entrants (RADIUS).

0b A titre facultatif, l'utilisateur s'enregistre auprès du serveur d'application web/WAP. Son identifiant est associé à un ou plusieurs numéros MSISDN.

1 L'utilisateur envoie une requête pour rechercher un service de proximité; l'un des champs de la requête contient son numéro MSISDN. Ce numéro peut être inséré par la passerelle WAP (comme décrit dans l'Appendice I.1.1) ou renseigné par l'utilisateur lui-même et vérifié par le serveur selon une procédure qui sort du champ de la présente Recommandation.

2 Le serveur WAP/web analyse la requête et en extrait le numéro MSISDN; il envoie ensuite à la passerelle AUG une requête contenant le numéro MSISDN en invoquant l'API «obtenir la géolocalisation».

3 La passerelle AUG met en correspondance le numéro MSISDN (identifiant service) et l'identité IMSI (identifiant réseau).

4 La passerelle AUG interroge le coeur de réseau pour connaître l'emplacement actuel correspondant à l'identité IMSI.

5 Le coeur de réseau prend contact avec l'équipement d'utilisateur correspondant à l'identité IMSI et finalise la mise à jour de la géolocalisation.

6 Le coeur de réseau répond à la requête «obtenir la géolocalisation» envoyée par la passerelle AUG.

7 La passerelle AUG détermine le numéro MSISDN à partir de l'identité IMSI.

8 La passerelle AUG répond à la requête «obtenir la géolocalisation» envoyée par le serveur WAP/web.

9 Le serveur WAP/web répond à la requête de l'utilisateur (recherche d'un service de proximité) en utilisant les données de localisation renvoyées par le réseau, et montre les résultats de la recherche à l'utilisateur.

Bibliographie

[IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Protocole d'ouverture de session (SIP: Session Initiation Protocol).*

[IETF RFC 4186] IETF RFC 4186 (2006), *Méthode de protocole d'authentification extensible pour les modules d'identité (EAP-SIM) des abonnées au Système mondial de communications mobiles (GSM) (Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)).*

[3GPP TS 33.328] 3GPP TS 33.328 V12.6.0 (2014), *IP Multimedia Subsystem (IMS) media plane security (Release 12).*

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	**Organisation du travail de l'UIT-T**
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
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
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changements climatiques, déchets d'équipements électriques et électroniques, efficacité énergétique, 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 et mesures et tests associés
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, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2017