Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2721

(09/2010)

SÉRIE Y: INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

Réseaux de prochaine génération – Sécurité

Spécifications et cas d'utilisation de la gestion d'identité dans les réseaux NGN

Recommandation UIT-T Y.2721

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
Télévision IP sur réseaux de prochaine génération	Y.1900–Y.1999
RÉSEAUX DE PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
Numérotage, nommage et adressage	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Réseaux de transmission par paquets	Y.2600–Y.2699
Sécurité	**Y.2700–Y.2799**
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999
RÉSEAUX FUTURS	Y.3000–Y.3499
INFORMATIQUE EN NUAGE	Y.3500–Y.3999

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

Recommandation UIT-T Y.2721

Spécifications et cas d'utilisation de la gestion d'identité dans les réseaux NGN

Résumé

La Recommandation UIT-T Y.2721 présente des exemples de cas d'utilisation et les spécifications de la gestion d'identité (IdM) dans les réseaux de prochaine génération (NGN) et au niveau de leurs interfaces. Les fonctions et capacités de gestion IdM sont utilisées pour accroître la confiance dans les informations d'identité ainsi que pour prendre en charge et améliorer des applications commerciales et liées à la sécurité, y compris des services fondés sur l'identité.

Les spécifications définies dans cette Recommandation sont destinées aux réseaux NGN (c'est-à-dire aux réseaux gérés en mode paquet), tels que définis dans la Recommandation UIT-T Y.2001.

Les objectifs et spécifications exposés dans cette Recommandation reposent sur le cadre de gestion d'identité défini dans la Recommandation UIT-T Y.2720 ainsi que sur une analyse d'exemples de cas d'utilisation applicables aux réseaux NGN. Ces exemples de cas d'utilisation, donnés à titre d'information, sont décrits dans les appendices de cette Recommandation.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T Y.2721	2010-09-16	13

Mots clés

Gestion d'identité, identité fédérée, réseau de prochaine génération, sécurité.

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 Y.2721

Spécifications et cas d'utilisation de la gestion d'identité dans les réseaux NGN

1 Domaine d'application

La présente Recommandation contient les objectifs, spécifications et lignes directrices concernant la gestion d'identité (IdM) dans les réseaux de prochaine génération (NGN) et au niveau de leurs interfaces et donne des exemples de cas d'utilisation. Les fonctions et capacités de gestion IdM sont utilisées pour accroître la confiance dans les informations d'identité, ainsi que pour prendre en charge et améliorer des applications commerciales et liées à la sécurité, y compris des services fondés sur l'identité.

Les objectifs, spécifications, lignes directrices et exemples de cas d'utilisation figurant dans la présente Recommandation portent notamment sur ce qui suit:

- L'accroissement de la confiance dans les informations d'identité d'une entité NGN (par exemple, utilisateur, groupe, dispositif d'utilisateur, fournisseur de service, entreprise, fédération, élément de réseau ou objet).
- La gestion sécurisée du cycle de vie (par exemple enregistrement, validation, révocation) des informations d'identité sous réserve du consentement spécifique et éclairé de l'utilisateur.
- La gestion d'identité au service des applications commerciales (par exemple authentification unique et déconnexion unique pour plusieurs services d'application) et des applications liées à la sécurité (par exemple contrôles d'accès), y compris des services fondés sur l'identité (par exemple authentification, assertions et identité fédérée).
- La découverte et l'échange sécurisés d'informations associées à l'identité ou aux identités d'une entité NGN sous réserve du consentement spécifique et éclairé de l'utilisateur. Ces informations peuvent être situées à l'intérieur d'un réseau NGN ou à travers différents domaines administratifs ou fédérations.
- L'interfonctionnement/interopérabilité entre les systèmes et les capacités de gestion IdM à l'intérieur du domaine d'un fournisseur NGN (c'est-à-dire intraréseau).
- L'interfonctionnement/interopérabilité des systèmes et des capacités de gestion IdM entre différents domaines de fournisseur ou fédérations sous réserve du consentement spécifique et éclairé de l'utilisateur en ce qui concerne les informations d'utilisateur (par exemple entre fournisseurs NGN, fournisseurs de services web et fournisseurs de contenus).
- La mise en application des politiques applicables (par exemple protection des informations d'identification personnelle) associées à l'identité ou aux informations d'identité d'une entité.
- La sécurité des systèmes, fonctions, capacités, données et communications de gestion IdM.

Les objectifs et spécifications énoncés dans la présente Recommandation sont destinés aux réseaux NGN (c'est-à-dire aux réseaux gérés en mode paquet), tels que définis dans [UIT-T Y.2001], *Aperçu général des réseaux de prochaine génération*.

Les objectifs et spécifications exposés dans la présente Recommandation reposent sur le cadre de gestion d'identité défini dans [UIT-T Y.2720] et sur une analyse des exemples de cas d'utilisation décrits dans les appendices.

NOTE 1 – Dans la présente Recommandation, le terme "identité" employé en relation avec la gestion d'identité n'est pas utilisé dans son acception absolue. En particulier, il ne renvoie pas à la validation positive d'une personne.

NOTE 2 – Dans la présente Recommandation, un utilisateur peut être une personne. Il peut désigner une personne, un groupe, une entreprise, une entité juridique, ou toute autre entité qui utilise des services NGN.

NOTE 3 – Dans la présente Recommandation, le terme "fournisseur de service d'identité/NGN (fournisseur IdSP/NGN)" est utilisé pour indiquer que le fournisseur de services IdM pourrait être un fournisseur NGN ou une tierce partie.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. 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 E.107] Recommandation UIT-T E.107 (2007), *Service de télécommunications d'urgence (ETS) et cadre d'interconnexion pour applications nationales du service ETS*.

[UIT-T X.811] Recommandation UIT-T X.811 (1995) | ISO/CEI 10181-2:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'authentification.*

[UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité*.

[UIT-T Y.2001] Recommandation UIT-T Y.2001 (2004), *Aperçu général des réseaux de prochaine génération.*

[UIT-T Y.2012] Recommandation UIT-T Y.2012 (2010), *Prescriptions et architecture fonctionnelles du réseau de prochaine génération.*

[UIT-T Y.2201] Recommandation UIT-T Y.2201 (2009), *Spécifications et capacités des réseaux de prochaine génération de l'UIT-T.*

[UIT-T Y.2205] Recommandation UIT-T Y.2205 (2008), *Réseaux de prochaine génération – Télécommunications d'urgence – Considérations techniques*.

[UIT-T Y.2702] Recommandation UIT-T Y.2702 (2008), *Spécifications d'authentification et d'autorisation pour les réseaux de prochaine génération version 1*.

[UIT-T Y.2720] Recommandation UIT-T Y.2720 (2009), *Cadre de gestion d'identité dans les NGN*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 anonymat [UIT-T X.1252]: situation dans laquelle une entité ne peut pas être identifiée parmi un ensemble d'entités.

NOTE – L'anonymat permet d'empêcher le traçage d'entités ou de leur comportement (emplacement de l'utilisateur, fréquence d'utilisation d'un service, etc.).

3.1.2 assertion [UIT-T X.1252]: affirmation faite par une entité non accompagnée d'une preuve de validité.

3.1.3 attribut [UIT-T X.1252]: information liée à une entité qui en spécifie une caractéristique.

3.1.4 authentification [UIT-T X.1252]: processus utilisé pour obtenir une confiance suffisante dans le lien entre l'entité et l'identité présentée.

NOTE – Dans un contexte de gestion d'identité (IdM), le terme authentification désigne l'authentification d'entité.

3.1.5 garantie d'authentification [UIT-T X.1252]: degré de confiance obtenu dans le processus d'authentification, dans le fait que le partenaire de communication est l'entité qu'il déclare être ou qu'il est censé être.

NOTE – La confiance repose sur le degré de confiance dans le lien entre l'entité communicante et l'identité présentée.

3.1.6 autorisation [UIT-T X.1252]: octroi de droits et octroi d'accès sur la base de ces droits.

3.1.7 lien [UIT-T X.1252]: association, rapport ou relation explicite établi.

3.1.8 déclaration [UIT-T X.1252]: affirmer être le cas, sans pouvoir fournir de preuve.

3.1.9 déclarant [UIT-T X.1252]: entité qui est ou représente une entité principale à des fins d'authentification.

NOTE – Un déclarant comporte les fonctions nécessaires pour engager des échanges pour authentification au nom d'une entité principale.

3.1.10 contexte [UIT-T X.1252]: environnement avec des frontières définies dans lequel des entités existent et interagissent.

3.1.11 justificatif [UIT-T X.1252]: ensemble de données présentées comme preuve d'une identité déclarée et/ou de droits.

3.1.12 délégation [UIT-T X.1252]: action d'attribuer une autorité, une responsabilité ou une fonction à une autre entité.

3.1.13 découverte [UIT-T Y.2720]: acte de localiser une description, exploitable par une machine, d'une ressource réseau qui pouvait être inconnue auparavant et qui satisfait certains critères fonctionnels. Elle nécessite le recoupement d'un ensemble de critères fonctionnels et d'autres natures avec un ensemble de descriptions de ressource. L'objectif est de trouver une ressource de service adaptée.

3.1.14 entité [UIT-T X.1252]: élément qui a une existence séparée et distincte et peut être identifié dans un contexte.

NOTE – Une entité peut être une personne physique, un animal, une personne morale, une organisation, une chose active ou passive, un dispositif, une application logicielle, un service, etc., ou un groupe de ces entités. Dans le contexte des télécommunications, il peut s'agir de points d'accès, d'abonnés, d'utilisateurs, d'éléments de réseau, de réseaux, d'applications logicielles, de services et de dispositifs, d'interfaces, etc.

3.1.15 télécommunications d'urgence (ET, *emergency telecommunications*) [UIT-T Y.2205]: tout service associé à une urgence qui nécessite un traitement spécial de la part du réseau NGN par rapport aux autres services. Les télécommunications d'urgence comprennent les services de sécurité du public et les services d'urgence autorisés par les pouvoirs publics.

3.1.16 service de télécommunications d'urgence (ETS, *emergency telecommunications service*) [UIT-T E.107]: service national offrant des télécommunications prioritaires aux utilisateurs autorisés en cas de catastrophe et de situation d'urgence.

3.1.17 fédération [UIT-T X.1252]: association d'utilisateurs, de fournisseurs de service et de fournisseurs de service d'identité.

3.1.18 identité fédérée [UIT-T Y.2720]: identité qui peut être utilisée pour accéder à un groupe de services ou d'applications défini selon les politiques et conditions d'une fédération.

3.1.19 identificateur [UIT-T X.1252]: un ou plusieurs attributs utilisés pour identifier une entité dans un contexte.

NOTE – Dans le contexte des réseaux NGN tel que défini dans [b-UIT-T Y.2091], un identificateur est une suite de chiffres, de caractères, de symboles ou de toute autre forme de données, utilisée pour identifier un ou plusieurs abonnés, utilisateurs, éléments de réseau, fonctions, entités de réseau fournissant des services ou des applications, ou d'autres entités (par exemple des objets physiques ou logiques).

3.1.20 identité [UIT-T X.1252]: représentation d'une entité sous la forme d'un ou de plusieurs attributs qui sont suffisants pour pouvoir distinguer les entités dans un contexte. Aux fins de la gestion d'identité (IdM), le terme identité désigne l'identité contextuelle (sous-ensemble d'attributs), c'est-à-dire que la diversité des attributs est limitée par un cadre avec des frontières définies (le contexte) dans lequel l'entité existe et interagit.

NOTE – Chaque entité est représentée par une identité holistique, qui comprend tous les éléments d'information possibles caractérisant cette entité. Toutefois, l'identité holistique est théorique et échappe à toute description et utilisation pratique, car le nombre de tous les attributs possibles est indéfini.

3.1.21 garantie d'identité [UIT-T X.1252]: degré de confiance dans le processus de validation et de vérification d'identité utilisé pour établir l'identité de l'entité à laquelle le justificatif a été délivré, et degré de confiance dans le fait que l'entité qui utilise le justificatif est cette entité ou l'entité à laquelle le justificatif a été délivré ou attribué.

3.1.22 gestion d'identité [UIT-T Y.2720]: ensemble de fonctions et de capacités (par exemple, l'administration, la gestion et la tenue à jour, la découverte, les échanges de communication, la corrélation et les liens, l'application des politiques, l'authentification et les assertions) utilisées pour:

- garantir les informations d'identité (par exemple, les identificateurs, les justificatifs, les attributs),
- garantir l'identité d'une entité (par exemple les utilisateurs/abonnés, les groupes, les dispositifs d'utilisateur, les organisations, les fournisseurs de réseaux et de services, les éléments et objets de réseaux et les objets virtuels), et
- permettre des applications commerciales et liées à la sécurité.

3.1.23 profil d'identité [UIT-T X.1252]: expression structurée d'attributs d'une entité (par exemple le comportement d'une entité) qui pourrait être utilisée dans certains processus d'identification.

3.1.24 fournisseur d'identité: Voir fournisseur de service d'identité (IdSP).

NOTE – Le terme "fournisseur d'identité (IdP)" est employé dans [UIT-T Y.2720] et dans des spécifications d'autres organisations. Toutefois, pour éviter que ce terme soit interprété à tort comme désignant une entité qui fournit des identités, et non comme une entité qui gère des identités, c'est le terme "fournisseur de service d'identité (IdSP)" qui est employé dans la présente Recommandation.

3.1.25 fournisseur de service d'identité [UIT-T X.1252]: entité qui vérifie, tient à jour, gère et peut créer et attribuer des informations d'identité d'autres entités.

3.1.26 réseau de prochaine génération [UIT-T Y.2001]: réseau en mode paquet, en mesure d'assurer des services de télécommunication et d'utiliser de multiples technologies de transport à large bande à qualité de service imposée et dans lequel les fonctions liées aux services sont indépendantes des technologies sous-jacentes liées au transport. Il assure le libre accès des utilisateurs aux réseaux et aux services ou fournisseurs de services concurrents de leur choix. Il prend en charge la mobilité généralisée qui permet la fourniture cohérente et partout à la fois des services aux utilisateurs.

3.1.27 information d'identification personnelle (PII, *personally identifiable information*) [UIT-T X.1252]: toute information: a) identifiant ou permettant d'identifier la personne à laquelle elle se rapporte, de se mettre en rapport avec elle ou de la localiser; b) permettant d'obtenir des informations d'identification ou les coordonnées d'une personne; ou c) étant ou pouvant être directement ou indirectement liée à une personne physique.

3.1.28 présence [UIT-T Y.2720]: ensemble d'attributs qui caractérisent une entité en relation avec le statut actuel.

3.1.29 entité principale [UIT-T X.811]: entité dont l'identité peut être authentifiée.

3.1.30 respect de la vie privée [UIT-T X.1252]: droit des individus de contrôler ou d'agir sur les informations les concernant qui peuvent être collectées, gérées, conservées, consultées et utilisées ou distribuées.

3.1.31 partie utilisatrice (RP, *relying party*) [UIT-T Y.2720]: entité qui est tributaire d'une représentation ou d'une déclaration d'identité soumise par une entité requérante/assertante dans un contexte de demande donné.

3.1.32 domaine de sécurité [UIT-T X.1252]: ensemble d'éléments, politique de sécurité, autorité de sécurité et ensemble d'activités liées à la sécurité dont les éléments sont gérés conformément à la politique de sécurité.

3.1.33 confiance [UIT-T X.1252]: conviction que des informations sont fiables et vraies ou qu'une entité est apte et disposée à agir de façon appropriée dans un contexte spécifié.

3.1.34 utilisateur [UIT-T X.1252]: toute entité qui utilise une ressource, par exemple un système, un équipement, un terminal, un processus, une application ou un réseau d'entreprise.

NOTE – Dans le contexte des réseaux NGN, conformément à [b-UIT-T Y.2091], un utilisateur est un utilisateur final, une personne, un abonné, un système, un équipement, un terminal (par exemple un télécopieur ou un PC), une entité (fonctionnelle), un processus, une application, un fournisseur ou un réseau d'entreprise.

3.1.35 vérificateur [UIT-T X.1252]: entité qui vérifie et valide des informations d'identité.

3.2 Termes définis dans la présente Recommandation

Aucun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations suivantes:

3G	3ème génération
AKA	authentification et concordance de clés (*authentification and key agreement*)
ANI	interface application-réseau (*application-to-network interface*)
API	interface de programmation d'application (*application programming interface*)
BSS	système d'appui aux activités (*business support system*)
CSP	fournisseur de service de communication (*communications service provider*)
DDoS	déni de service réparti (*distributed denial of service*)
DeviceID	identité de dispositif, ID de dispositif (*device identity*)
DoS	déni de service (*denial of service*)
EAG	passerelle pour les applications externes (*external application gateway*)
EDS	service d'annuaire d'entreprise (*enterprise directory service*)

ET	télécommunications d'urgence (*emergency telecommunications*)
ETS	service de télécommunications d'urgence (*emergency telecommunications service*)
EV-DO	technologie évoluée – données optimisées (*evolution data optimized*)
FE	entité fonctionnelle (*functional entity*)
FTTX	fibre jusqu'à X (*fibre-to-the-X*)
GBA	architecture d'amorçage générique (*generic bootstrapping architecture*)
HSS	serveur d'abonnés de rattachement (*home subscriber server*)
IBGC-FE	entité fonctionnelle de contrôle de passerelle frontière d'interconnexion (*interconnection border gateway control functional entity*)
IdM	gestion d'identité (*identity management*)
IdMCC-FE	entité fonctionnelle de coordination et de contrôle de gestion d'identité (*IdM coordination and control functional entity*)
IdSP	fournisseur de service d'identité (*identity service provider*)
IDPS	système de détection et de prévention des intrusions (*intrusion detection and prevention system*)
ID-WSF	cadre des services web d'identité (*identity web services framework*)
IMS	sous-système multimédia IP (*IP multimedia subsystem*)
IP	protocole Internet (*Internet protocol*)
ISC	commande de service IMS (*IMS service control*)
IT	technologies de l'information (*information technology*)
KDC	centre de distribution de clés (*key distribution centre*)
LS	serveur de localisation (*location server*)
LTE	évolution à long terme (*long term evolution*)
MNO	opérateur de réseau mobile (*mobile network operator*)
MSISDN	numéro d'annuaire de l'abonné mobile pour les services intégrés (*mobile subscriber integrated service directory number*)
NACF	fonction de commande de rattachement au réseau (*network attachment control function*)
NGN	réseau de prochaine génération (*next generation network*)
NNI	interface réseau-réseau (*network-to-network interface*)
OAM&P	exploitation, administration, maintenance et approvisionnement (*operation, administration, maintenance and provisioning*)
OSS	système d'appui à l'exploitation (*operations support system*)
PC	ordinateur personnel (*personal computer*)
P-CSC-FE	entité fonctionnelle proxy de commande de session d'appel (*proxy call session control functional entity*)
PDA	assistant numérique personnel (*personal digital assistant*)
PII	informations d'identification personnelle (*personally identifiable information*)
POTS	système téléphonique ordinaire (*plain old telephone system*)

PS serveur de présence (*presence server*)

QoS qualité de service (*quality of service*)

RACF fonction de contrôle des ressources et d'admission (*resource and admission control function*)

RFID identification par radiofréquence (*radio-frequency identification*)

RP partie utilisatrice (*relying party*)

RTPC réseau téléphonique public commuté

SAA-FE entité fonctionnelle d'authentification et d'autorisation pour un service (*service authentification and autorization functional entity*)

SAML langage de balisage d'assertion de sécurité (*security assertion markup language*)

S-CSC-FE entité fonctionnelle serveur de commande de session d'appel (*serving call session control functional entity*)

SIM module d'identité d'abonné (*subscriber identity module*)

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

SLA accord de niveau de service (*service level agreement*)

SN nœud de service (*service node*)

SNI interface serveur-réseau (*server-to-network interface*)

SP fournisseur de service (*service provider*)

SUP-FE entité fonctionnelle de profil d'utilisateur pour un service (*service user profile functional entity*)

TGS serveur distributeur de tickets (*ticket granting server*)

TVIP télévision IP

UE équipement d'utilisateur (*user equipment*)

UICC carte de circuits intégrés universelle (*universal integrated circuit card*)

UNI interface utilisateur-réseau (*user-to-network interface*)

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

UserID identité d'utilisateur, ID d'utilisateur (*user identity*)

VoD vidéo à la demande (*video on demand*)

VoIP téléphonie IP (*voice over Internet protocol*)

WiFi fidélité sans fil (*wireless fidelity*)

WiMAX interopérabilité mondiale pour l'accès hyperfréquences (*worldwide interoperability for microwave access*)

WLAN réseau local sans fil (*wireless local area network*)

WS serveur web (*web server*)

WSG passerelle pour les services web (*web services gateway*)

xDSL boucle d'abonné numérique x (*x digital subscriber loop*)

5 Conventions

Dans la présente Recommandation:

L'expression "**il est obligatoire**" indique une spécification qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**il est recommandé**" indique une spécification qui est recommandée mais qui n'est pas absolument nécessaire. Cette disposition n'est donc pas indispensable pour déclarer la conformité.

L'expression "**il est interdit**" indique une spécification qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**peut, à titre d'option**" indique une spécification optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant d'implémenter l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de service de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité à la présente Recommandation.

Dans le corps de la présente Recommandation et dans ses annexes, on trouve parfois les expressions *doit*, *ne doit pas*, *devrait* et *peut*. Celles-ci doivent respectivement être interprétées comme correspondant aux expressions *il est obligatoire*, *il est interdit*, *il est recommandé* et *peut, à titre d'option*. Lorsque ces expressions apparaissent dans un appendice ou dans des parties dans lesquelles il est expressément indiqué qu'elles sont *données à titre d'information*, elles doivent être interprétées comme étant dépourvues d'intention normative.

6 Présentation de la gestion d'identité

6.1 Considérations générales

[UIT-T Y.2720] définit un cadre pour la gestion d'identité (IdM). Les fonctions et capacités de gestion IdM sont utilisées pour accroître la confiance dans les informations d'identité d'une entité, ainsi que pour prendre en charge des applications commerciales et liées à la sécurité (par exemple contrôle d'accès et autorisation), y compris des services fondés sur l'identité. Une entité est considérée comme étant tout type d'élément qui a une existence séparée et distincte et peut être identifié dans un contexte. Dans le contexte de la gestion IdM, il peut s'agir d'abonnés, d'utilisateurs, d'éléments de réseaux, de réseaux, d'applications logicielles, de services et de dispositifs.

Les réseaux NGN prendront en charge une grande variété de services d'application pour les utilisateurs finals, les pouvoirs publics et les entreprises privées. Afin d'assurer la protection de l'intégrité et de la sécurité des services d'application, il est recommandé que les réseaux NGN prennent en charge les fonctions et capacités nécessaires pour garantir l'identité et les données d'identité associées à une entité sur la base d'un contexte spécifique. La gestion IdM est définie dans [UIT-T X.1252].

Les exemples de cas d'utilisation décrits dans les appendices suivants sont pris en considération pour définir les spécifications de gestion IdM:

- Appendice I – Cas d'utilisation généraux de la gestion IdM
- Appendice II – Cas d'utilisation de la gestion IdM pour les applications NGN
- Appendice III – Cas d'utilisation de la gestion IdM liés au service de télécommunication d'urgence (ETS)

- Appendice IV – Cas d'utilisation liés au mobile.

De plus, les facteurs suivants associés aux identités d'utilisateur final dans un environnement NGN sont pris en considération pour définir les spécifications de gestion IdM:

- Les utilisateurs finals utilisent de plus en plus des identités multiples.
- Une identité peut être associée à différents contextes et privilèges de service.
- Il se peut qu'une identité n'identifie un utilisateur final que partiellement.
- Des pseudonymes peuvent être utilisés comme identité.
- Des identités peuvent être utilisées n'importe où, à tout moment et depuis n'importe quel dispositif.
- Il est possible que des identités ne soient pas compatibles entre différents fournisseurs NGN.

6.2 Relations de gestion IdM

La Figure 1 donne un aperçu général des relations de gestion IdM sur la base du cadre contenu dans [UIT-T Y.2720].

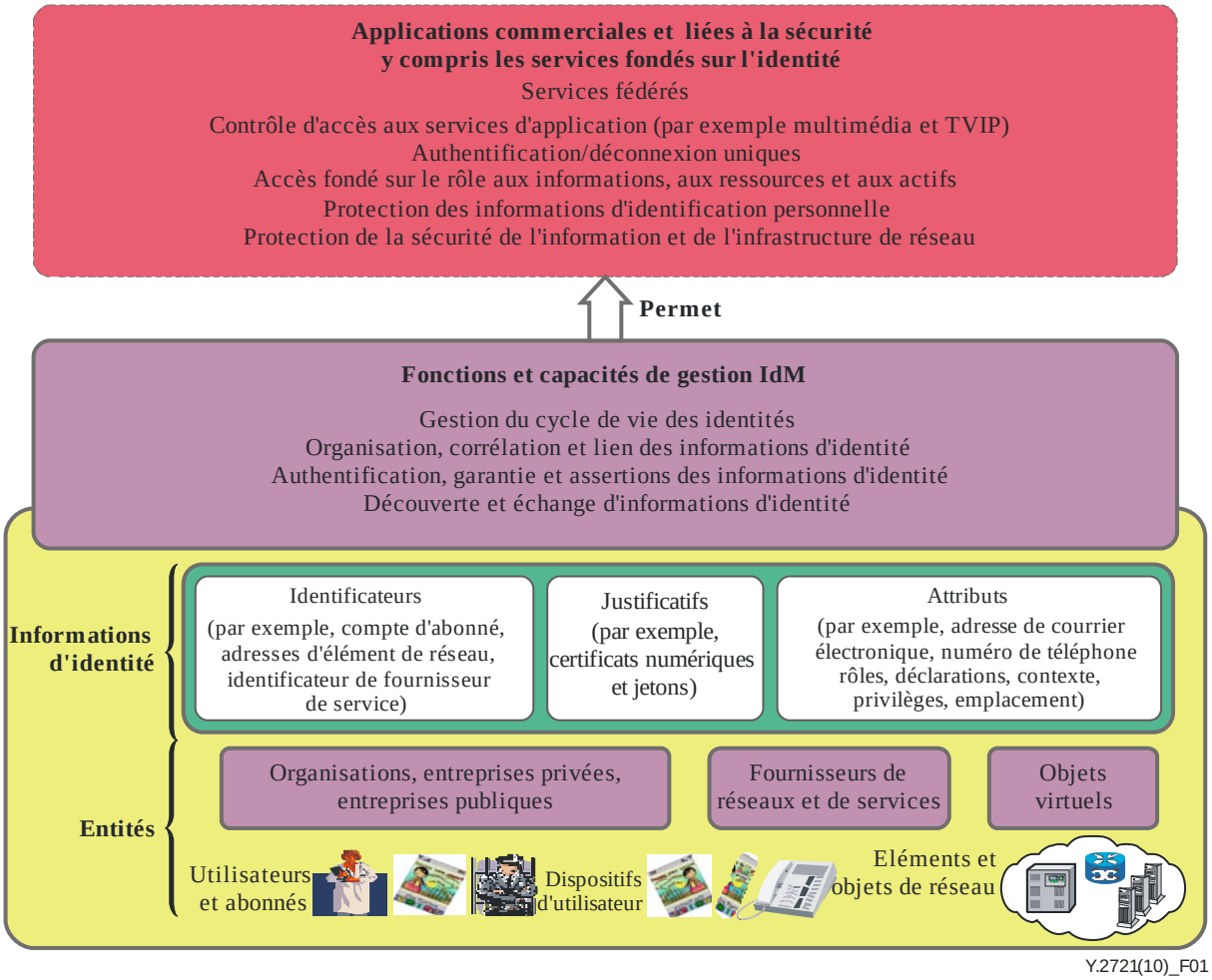


Figure 1 – Relations de gestion IdM

Parmi les entités, on trouve des utilisateurs humains individuels, de vastes organisations (par exemple des entreprises) ou encore des objets virtuels (par exemple des applications électroniques). Du point de vue de la sensibilité, les informations d'identité associées à chaque entité vont de données relativement publiques (par exemple un numéro de téléphone figurant dans un annuaire

public) à des données d'identité très sensibles (par exemple des mots de passe, des certificats numériques et d'autres authentificateurs privés).

Une entité peut avoir une ou plusieurs identités, qui peuvent être utilisées pour représenter plusieurs rôles (par exemple citoyen, conjoint, parent, client et patient) et pour réaliser des transactions spécifiques dans différents domaines commercial, social, etc.). Une personne ou un particulier peut être associé à plusieurs identités numériques en fonction du contexte comme indiqué sur la Figure 1. De plus, une personne qui agit en utilisant des identités numériques peut être connue des autres comme étant quelqu'un qui remplit une ou plusieurs fonctions supposées ou affichées en public ou dans la société, ou qui remplit des rôles (par exemple, personne chargée d'intervenir en cas d'urgence) attribués ou octroyés par une certaine autorité.

Les éléments apparaissant sur la Figure 1 sont les suivants:

a) Entités:

Dans un environnement NGN dans lequel les services sont fondés sur des contextes et des rôles et sont accessibles n'importe où, à tout moment et depuis n'importe quel dispositif, plusieurs formes d'informations relatives aux identités peuvent être associées à une entité. De plus, une entité peut avoir une ou plusieurs identités en fonction du contexte. Comme exemples d'entités, on peut citer:

- Les utilisateurs et les abonnés.
- Les dispositifs d'utilisateur, éléments et objets de réseau.
- Les organisations, groupes, entreprises privées et structures de l'Etat.
- Les fournisseurs de réseau et de service.
- Les objets virtuels.

b) Informations d'identité

Les informations d'identité associées à une entité peuvent être regroupées de la manière suivante:

- Identificateurs (par exemple compte d'abonné, adresses d'élément de réseau, identificateur de fournisseur de service).
- Attributs (par exemple adresses de courrier électronique, numéros de téléphone, identificateurs URI, et adresses IP, rôles, déclarations, privilèges, méthode d'authentification, profils et emplacement).
- Justificatifs (par exemple certificats numériques et jetons.

c) Fonctions et capacités de gestion IdM

Les fonctions et capacités de gestion IdM sont utilisées pour accroître la confiance dans les informations d'identité d'une entité et prendre en charge ou améliorer des applications commerciales et liées à la sécurité, y compris des services fondés sur l'identité. Comme exemples de fonctions et de capacités de gestion IdM, on peut citer:

- La gestion du cycle de vie des identités.
- L'organisation, la corrélation et le lien des informations d'identité.
- L'authentification, la garantie d'authentification et l'assertion.
- La découverte et l'échange d'informations d'identité.
- Les fonctions et capacités de relais entre différents systèmes de gestion IdM pour faciliter l'interopérabilité.

d) Applications commerciales et liées à la sécurité

Les fonctions et capacités de gestion IdM prennent en charge et améliorent des applications commerciales et liées à la sécurité, y compris des services fondés sur l'identité.

Comme exemples d'applications commerciales, on peut citer:

- Les services fédérés (par exemple accès à des services à travers différentes fédérations ou différents fournisseurs NGN).
- L'authentification et la déconnexion uniques (par exemple accès à de multiples applications et services sans avoir à soumettre à nouveau les justificatifs d'authentification à chaque plate-forme d'application ou de service).

Comme exemples d'applications liées à la sécurité, on peut citer:

- Le contrôle d'accès
- La gestion d'autorisation des privilèges.
- La protection des informations d'identification personnelle (PII).

Comme exemples de services fondés sur l'identité, on peut citer:

- Les services d'identificateurs, de justificatifs et d'attributs.
- Les services de relais (correspondance et interfonctionnement des informations d'identité dans un environnement hétérogène).
- Les services d'informations de profil.

La gestion IdM inclut des processus de gestion du cycle de vie, plus les fonctions et les capacités nécessaires pour découvrir et obtenir les sources d'identité qui peuvent être utilisées pour vérifier et valider une identité. Les services et capacités de gestion IdM permettent aux entités de contrôler la manière dont leurs informations d'identité sont utilisées et diffusées. La gestion IdM fournit aux entités (par exemple parties utilisatrices) les informations nécessaires pour prendre des décisions concernant l'authentification et avoir confiance dans les transactions et communications associées. La gestion IdM permet aussi aux membres d'une fédération (par exemple différents fournisseurs NGN, entreprises privées ou structures de l'Etat) d'échanger et d'utiliser des informations d'identité fédérée afin de prendre en charge des services fédérés. Ces services pourraient par exemple permettre aux entités autorisées des membres de la fédération d'obtenir un accès à des ressources sur la base de rôles et de privilèges conformément aux règles et aux politiques de la fédération sans qu'il soit nécessaire de procéder à un enregistrement et à une authentification auprès de chaque membre de la fédération.

6.3 Besoins et justification

Etant donné qu'un grand nombre de services et de capacités NGN reposent sur un service basé sur l'identité et les préférences de l'abonné et sur un accès depuis n'importe quel dispositif, n'importe où et à tout moment, les solutions de gestion IdM doivent permettre de faire face en temps réel à des interactions de plus en plus complexes liées au fait que les utilisateurs peuvent passer d'un dispositif à un autre, d'une technologie d'accès à une autre, d'une méthode de paiement à une autre voire d'une identité à une autre. De plus, les utilisateurs finals souhaitent disposer de capacités faciles à utiliser et, surtout, ils souhaitent disposer de capacités leur permettant d'avoir le contrôle de la confidentialité et des informations d'identification personnelle (PII).

Les besoins et la justification de la gestion IdM viennent des utilisateurs finals (par exemple les abonnés des applications et des services), des fournisseurs NGN, des entreprises privées et des structures de l'Etat, tous souhaitant que leurs intérêts et besoins soient respectés par les mises en œuvre de la gestion IdM. Les facteurs suivants sont pris en considération pour définir les spécifications de gestion IdM pour les réseaux NGN:

- Les utilisateurs finals/abonnés ont besoin de contrôler et de protéger leurs informations d'identité personnelle en ligne, souhaitent disposer de méthodes souples et uniformes d'accès aux ressources et ont besoin d'un juste équilibre entre les avantages des réseaux sociaux et l'exposition des informations personnelles.
- Les fournisseurs NGN (fournisseurs de réseau et de service) ont besoin de protéger les ressources de leurs infrastructures de réseau, leurs services et leurs applications, d'activer

des services fédérés, de promouvoir des services par abonnement largement disponibles et de répondre aux besoins des utilisateurs finals en matière de confidentialité et de protection des informations d'identification personnelle (PII).

- Les entreprises privées et les utilisateurs ont besoin de protéger leurs intérêts commerciaux, d'avoir confiance dans les capacités d'authentification pour les transactions commerciales et de protéger les données d'identité des partenaires commerciaux.
- Protection de l'infrastructure de réseau contre les cyberattaques et protection des données privées.
- Prise en charge par les organismes publics de services administratifs en ligne, de services de sécurité du public, de services d'alerte avancée, du service de télécommunications d'urgence (ETS) et d'autres services nationaux.

6.4 Environnement fédéré avec de multiples fournisseurs de service

Dans un environnement fédéré avec de multiples fournisseurs de service, les services et capacités de gestion IdM sont utilisés pour la découverte et la communication d'informations destinées à établir la confiance dans l'identité ou les identités d'une entité. A titre d'exemple, les identificateurs, justificatifs et attributs associés à une identité pourraient être vérifiés par un fournisseur de service d'identité considéré comme fiable par la partie utilisatrice et être communiqués, au moyen d'assertions, à la partie utilisatrice (par exemple un utilisateur, un fournisseur de service) afin d'assurer l'authentification nécessaire pour le contrôle d'accès, les décisions commerciales et la mise en application des politiques applicables (par exemple confidentialité et protection des informations d'identification personnelle).

Par ailleurs, il se peut qu'il existe différentes solutions de gestion IdM indépendantes, d'où la nécessité d'une interopérabilité entre les fournisseurs de service.

6.5 Fournisseur de service d'identité (IdSP)

La présente Recommandation n'impose aucune restriction quant à qui assure les services de fournisseur de service d'identité (IdSP).

Un fournisseur IdSP est une entité qui maintient, gère et peut créer des informations d'identité sécurisées pour d'autres entités (par exemple, utilisateurs/abonnés, organisations et dispositifs) et propose des services fondés sur l'identité basés sur une relation de confiance, commerciale ou d'autres natures.

Dans un environnement avec de multiples fournisseurs de service, un fournisseur NGN peut aussi être un fournisseur IdSP et offrir des services de gestion d'identité (par exemple, des services fondés sur l'identité) à d'autres fournisseurs.

Dans la présente Recommandation, le terme "fournisseur IdSP/NGN" est utilisé pour indiquer que le fournisseur de services IdM pourrait être un fournisseur NGN ou une tierce partie.

6.6 Gestion IdM dans le contexte du modèle d'architecture de référence des réseaux NGN

6.6.1 Relation avec l'architecture fonctionnelle des réseaux NGN

Dans le contexte du modèle d'architecture de référence des réseaux NGN défini dans [UIT-T Y.2012], les fonctions relatives à la gestion IdM peuvent résider dans les différents plans (par exemple utilisateur, commande et gestion) et dans les différentes strates de l'architecture répartie (par exemple strate des services et strate de transport). Du point de vue de la réalisation ou de la mise en œuvre, la prise en charge des services et capacités de gestion IdM pourrait reposer sur l'utilisation des éléments de réseau existants ou sur l'utilisation d'éléments de réseau supplémentaires (par exemple des serveurs d'application spécialisés) dans un réseau NGN.

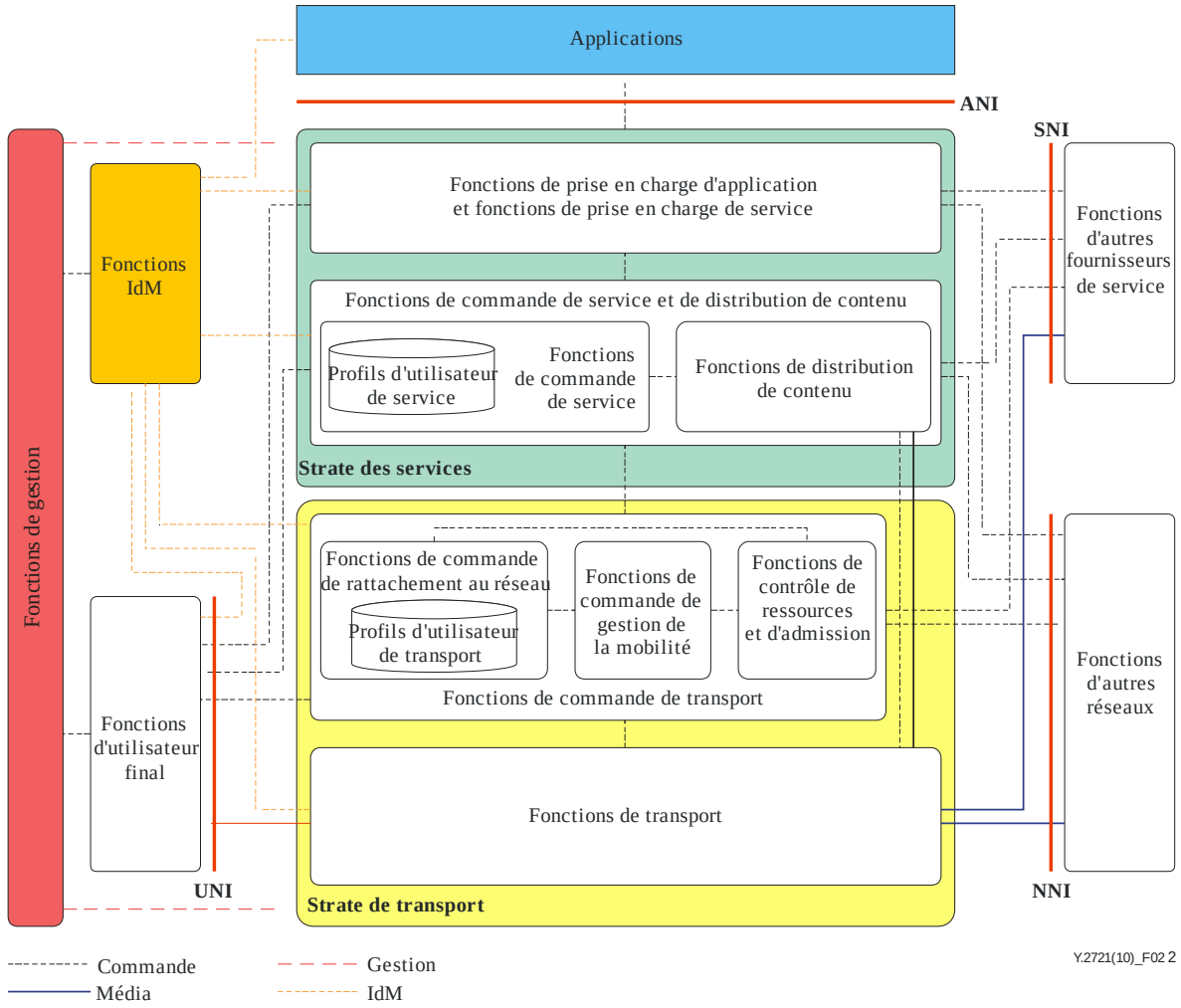


Figure 2 – Aperçu de l'architecture des réseaux NGN

La Figure 2, qui est basée sur la Figure 7-1 de [UIT-T Y.2012], comporte un bloc fonctionnel représentant les fonctions de gestion IdM dans l'architecture fonctionnelle des réseaux NGN. la Figure 7-1 de [UIT-T Y.2012] illustre d'une manière générale le fait que la prise en charge des services et capacités de gestion IdM peut entraîner une interaction avec des entités fonctionnelles spécifiques pour permettre la prise en charge de services, y compris de services d'identité. Des interactions sont notamment possibles avec des entités fonctionnelles des blocs fonctionnels suivants selon le service ou la capacité de gestion IdM spécifique prise en charge et la conception de la mise en œuvre:

– applications;

– strate des services: fonctions de prise en charge d'application et fonctions de prise en charge de service, fonctions de commande de service et fonctions de distribution de contenu;

– strate de transport: fonctions de commande de transport et fonctions de transport;

– fonctions d'utilisateur final;

– fonctions de gestion.

Dans l'architecture fonctionnelle des réseaux NGN, les fonctions de gestion IdM peuvent résider dans différents plans (par exemple utilisateur, commande et gestion) et différentes strates de l'architecture répartie (par exemple strate des services et strate de transport). La représentation des

fonctions de gestion IdM dans un groupe de fonctions autonome ne vise à imposer aucune conception et aucune restriction particulières concernant les mises en œuvre de la gestion IdM. La mise en œuvre de fonctions de gestion IdM doit se faire dans le respect des politiques applicables, par exemple les réglementations et législations nationales et régionales en matière de protection des données d'identité (par exemple les informations PII). En particulier, la mise en œuvre et l'utilisation de fonctions de gestion IdM doivent respecter les politiques applicables définissant les principes de base de la protection des données:

- rattachement des données à une finalité spécifique;
- pas de partage de données entre applications pour des finalités différentes;
- limitation des données au minimum nécessaire pour une finalité spécifique;
- droit des personnes d'avoir le contrôle de leurs informations PII.

NOTE – Dans le cadre de certaines réglementations nationales, il pourra être nécessaire de mettre en œuvre des fonctions de gestion IdM distinctes dans les différentes strates des réseaux NGN.

6.6.2 Interfaces externes et communications de gestion IdM

Les interfaces normalisées définies dans [UIT-T Y.2012] sont utilisées pour échanger des données d'identité entre différents domaines administratifs et différentes fédérations. Les interfaces peuvent notamment être les suivantes:

- interface utilisateur-réseau (UNI);
- interface réseau-réseau (NNI);
- interface application-réseau (ANI);
- interface serveur-réseau (SNI).

Les solutions retenues pour les interfaces dépendront normalement de facteurs tels que les besoins spécifiques des applications et des services (par exemple en temps réel ou quasiment en temps réel), le protocole utilisé (par exemple SAML, Diameter, RADIUS, SIP) et les mécanismes et méthodes.

On trouvera à l'Appendice VI un exemple de scénario de réalisation de la gestion IdM montrant comment les interfaces externes des réseaux NGN peuvent s'appliquer.

6.6.3 Modèles de transaction

[b-ITU-T X.1250] décrit des exemples de modèles de transaction faisant intervenir plusieurs parties (par exemple des utilisateurs, des fournisseurs IdSP et des parties utilisatrices). On trouvera à l'Appendice V une récapitulation des modèles de transaction décrits dans [b-UIT-T X.1250].

7 Objectifs de la gestion IdM

Les objectifs généraux de la gestion IdM sont les suivants:

1) Faciliter la prise de décisions en toute confiance entre les entités.
2) Prise en charge de solutions de gestion IdM affectant le moins possible les utilisateurs/abonnés.
3) Lorsqu'une ou plusieurs solutions reposent sur de nouvelles capacités, il faut prévoir une solution de transition appropriée.
4) Prise en charge de solutions de gestion IdM interopérables à l'intérieur du domaine d'un fournisseur NGN, par exemple, interopérabilité entre des produits de différents fournisseurs prenant en charge plusieurs services d'application (par exemple VoIP, TVIP, vidéo et données).
5) Prise en charge de solutions de gestion IdM interopérables à travers différents domaines de fournisseur NGN et de fournisseur de service et différentes fédérations sur la base des

relations et des accords commerciaux applicables et dans le respect de la réglementation et des politiques relatives à la protection des informations PII.

6) Prise en charge d'un relais entre les systèmes de gestion IdM hétérogènes et les fédérations, par exemple, capacité de mettre en place un relais entre les systèmes de gestion IdM de fournisseur NGN et d'autres types de systèmes de gestion IdM (par exemple, systèmes de gestion IdM de fournisseur de services web, de fournisseur de contenu et de fournisseur tiers) sur la base des relations et des accords commerciaux applicables et dans le respect de la réglementation et des politiques relatives à la protection des informations PII.

7) Capacité des utilisateurs finals/abonnés d'interagir et d'utiliser des services d'application facilement et de façon intuitive tout en conservant le contrôle de leurs données personnelles tout au long de leur cycle de vie. Les utilisateurs finals/abonnés doivent notamment pouvoir décider comment et quand les informations sont utilisées et par qui.

8) Capacité des utilisateurs finals/abonnés de ne révéler que les informations minimales nécessaires pour établir la confiance mutuelle et réaliser des transactions sur la base des politiques applicables.

9) Capacité des utilisateurs finals/abonnés de vérifier l'authenticité de l'entité demandant des données d'identité et des informations PII. Un utilisateur final/abonné doit pouvoir utiliser de multiples identificateurs en fonction du contexte.

10) Capacité des utilisateurs finals/abonnés d'agir anonymement, sous un pseudonyme ou sous leur propre nom, suivant le contexte de l'application et les politiques applicables.

8 Spécifications de gestion IdM

Le présent paragraphe décrit les spécifications de gestion IdM applicables aux réseaux NGN, compte tenu des spécifications de haut niveau des réseaux NGN décrites dans [UIT-T Y.2201].

8.1 Spécifications générales

Les spécifications générales relatives à la gestion d'identité sont les suivantes:

R-1 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des fonctions et des capacités pour la gestion d'identité des divers types d'entités prises en charge dans les réseaux NGN, à savoir:

a) les utilisateurs/groupes

b) les organisations/fédérations/entreprises/fournisseurs de service

c) les dispositifs/éléments de réseau/systèmes

d) les objets (par exemple processus d'application, contenus, données).

R-2 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge:

a) La gestion sécurisée du cycle de vie (par exemple de la délivrance à la révocation des identités).

b) La découverte et l'échange sécurisés d'informations d'identité, notamment la découverte et l'échange d'informations d'identité à l'intérieur d'un réseau NGN ou à travers différents domaines administratifs.

R-3 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge la mise en application des politiques applicables associées à l'identité ou aux informations d'identité d'une entité.

R-4 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des fonctions et des capacités de gestion IdM à la fois pour les applications en temps réel (par exemple VoIP et TVIP) et pour les applications quasiment en temps réel (par exemple transactions de données fondées sur le web).

R-5 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des fonctions et des capacités de gestion IdM permettant l'assertion anonyme d'informations d'identité (par exemple identité et attributs), sous réserve de la politique applicable.

R-6 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge un interfonctionnement sécurisé pour la gestion IdM entre éléments de réseau à l'intérieur du domaine d'un fournisseur NGN (c'est-à-dire intra-réseau) et entre les domaines de différents fournisseurs (par exemple un autre fournisseur NGN, des fournisseurs de services web).

R-7 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des services et des fonctionnalités destinés à faciliter l'utilisation par les utilisateurs finals comme:

a) l'authentification/déconnexion uniques pour plusieurs services d'application;

b) des services issus de la convergence (par exemple convergence fixe/mobile);

c) le contrôle et la protection des informations d'identification personnelle (PII).

R-8 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge l'authentification unique pour plusieurs applications sur la base des justificatifs associés à un dispositif d'abonné (par exemple les justificatifs UICC) ou des justificatifs à un utilisateur/abonné (par exemple les justificatifs SIP Digest), selon le cas, suivant la sécurité requise par les applications. En particulier:

- Il doit être possible d'utiliser des justificatifs d'abonné (par exemple les justificatifs SIP Digest) pour prendre en charge l'authentification unique pour l'accès à des applications via des dispositifs mobiles.
- Il doit être possible d'utiliser des justificatifs d'abonné (par exemple les justificatifs SIP Digest) pour prendre en charge l'authentification unique pour l'accès à des applications via des dispositifs fixes.

8.2 Spécifications de gestion du cycle de vie de l'identité

La gestion du cycle de vie de l'identité comprend les processus et procédures associés à l'inscription et à la délivrance d'informations d'identité (par exemple identificateurs, justificatifs et attributs).

R-9 Il est obligatoire que le fournisseur IdSP/NGN établisse et mette en application des politiques de gestion du cycle de vie de l'identité, et notamment des processus, procédures et politiques concernant le contrôle, l'inscription, la délivrance et la révocation d'informations d'identités.

8.2.1 Inscription et délivrance

Pour inscrire une entité (par exemple abonné, dispositif, organisation, fournisseur NGN ou objet) dans un contexte, on commence par contrôler et inscrire l'identité ou les justificatifs. L'inscription est le processus d'introduction d'une entité dans un contexte et consiste à enregistrer l'identité de l'entité et éventuellement à attribuer des attributs spécifiques (par exemple des identificateurs) ou des justificatifs ou des rôles. Dans le cas d'un utilisateur final, c'est le processus par lequel cet utilisateur final demande à s'abonner auprès d'un fournisseur IdSP ou d'un fournisseur NGN.

Le contrôle consiste à vérifier et à valider les attributs et les justificatifs éventuellement associés.

R-10 Il est obligatoire que le fournisseur IdSP/NGN vérifie et valide l'identité d'une entité lors de l'inscription conformément aux exigences du contexte. L'enregistrement de l'identité de l'entité et l'attribution d'identificateurs, de justificatifs et d'attributs pour le contexte spécifique sont subordonnés à la confirmation des critères et politiques de contrôle applicables.

Les processus et politiques de contrôle seront fondés sur la valeur des ressources (par exemple services, transactions, informations et privilèges) autorisées par l'identité et sur les

risques associés à l'obtention et à l'utilisation de l'identité par une entité non autorisée. Plus précisément, des mesures sont nécessaires pour garantir ce qui suit:

- une entité (par exemple une personne, une organisation ou une entité juridique) ayant les attributs déclarés existe et ces attributs permettent de distinguer suffisamment l'entité conformément aux besoins du contexte;
- un requérant dont l'identité est enregistrée est bien l'entité à laquelle l'identité est liée;
- il est difficile pour une entité qui a utilisé l'identité et les justificatifs enregistrés de répudier ultérieurement l'enregistrement/l'inscription et de contester une authentification.

L'achèvement avec succès du processus d'inscription et de contrôle se traduit par l'enregistrement de l'identité – et éventuellement des attributs et/ou des justificatifs attribués – qui permettra à l'entité de s'authentifier à l'avenir.

R-11 Il est obligatoire que les informations d'identité (par exemple les identificateurs, justificatifs et attributs) associées à une identité ne soient délivrées qu'après avoir contrôlé avec succès l'identité de l'entité.

Dans certains scénarios, il se peut que des justificatifs électroniques soient enregistrés et délivrés, par exemple des certificats et des jetons numériques se rapportant à une identité ou utilisés pour faire une déclaration (attribut) au sujet d'une identité. Suivant le type de jeton utilisé, le fournisseur IdSP/NGN créera un nouveau jeton et le fournira à l'abonné, ou demandera à l'abonné d'enregistrer un jeton que le requérant possède déjà ou a nouvellement créé.

R-12 Dans l'un ou l'autre cas, il est obligatoire de sécuriser le mécanisme de transport du jeton depuis la partie où il est créé jusqu'à l'autre partie pour faire en sorte que la confidentialité et l'intégrité du jeton nouvellement établi soient maintenues.

8.2.2 Maintien et mises à jour

Une fois qu'une ou plusieurs identités y compris d'éventuelles informations d'identité (identificateurs, justificatifs et attributs) ont été enregistrées et délivrées, le fournisseur IdSP/NGN et l'abonné sont chargés de les garder en sécurité pendant la phase d'utilisation opérationnelle.

R-13 Il est obligatoire que le fournisseur IdSP/NGN gère et maintienne en toute sécurité les données et le statut des données (par exemple identificateurs, justificatifs, attributs) associées à une identité.

R-14 Il est obligatoire que le fournisseur IdSP/NGN gère et journalise en toute sécurité les éventuelles mises à jour et modifications d'une identité.

R-15 Il est obligatoire que le fournisseur IdSP/NGN valide périodiquement le statut d'une identité.

R-16 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des procédures permettant de notifier les mises à jour et modifications d'une ou de plusieurs identités et des données associées, aux systèmes et éléments de réseau qui ont besoin d'être au courant des mises à jour et des modifications.

R-17 Il est obligatoire que le fournisseur IdSP/NGN dispose de fonctions permettant d'informer l'utilisateur au sujet de ses données d'identité et de modifier ou de supprimer ces données.

L'abonné est également responsable de la sécurité du justificatif attribué conformément aux accords commerciaux et politiques conclus avec le fournisseur IdSP/NGN. Par exemple, un abonné est chargé de gérer ses justificatifs électroniques (par exemple jetons) et de les garder en sécurité.

R-18 Il est obligatoire que le fournisseur IdSP/NGN prenne des mesures, sur la base d'accords commerciaux et contractuels, pour faire en sorte qu'une entité (par exemple un abonné ou un autre fournisseur IdSP/NGN) gère et utilise en toute sécurité les justificatifs délivrés (par

exemple jetons ou certificats numériques) associés à une identité sous réserve des réglementations et des politiques applicables.

8.2.3 Révocation

La révocation d'identité est le processus consistant à annuler une identité et les justificatifs associés. C'est la partie ou le système (par exemple fournisseur IdSP/NGN) qui gère l'identité ou les justificatifs qui est chargé de la révocation. La révocation est nécessaire afin d'empêcher qu'une identité ou qu'un justificatif qui n'est plus valable ou qui présente une faille de sécurité continue à être utilisé.

R-19 Il est obligatoire que le fournisseur IdSP/NGN établisse et mette en application des politiques de révocation d'identité. Plus précisément, des capacités doivent être prises en charge afin d'annuler ou de détruire les justificatifs (par exemple jetons ou certificats numériques) associés à une identité lorsque lesdits justificatifs ne sont plus valables ou qu'ils présentent une faille de sécurité.

R-20 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des procédures permettant de faire en sorte que la révocation ou l'annulation d'une ou de plusieurs identités et des données associées soit notifiée à l'entité et aux systèmes et éléments de réseaux qui ont besoin d'être au courant (autrement dit, tous les systèmes et processus avec lesquels l'identité peut être utilisée pour l'accès doivent être informés du fait que l'identité n'est plus valable).

8.3 Fonctions OAM&P relatives à la gestion d'identité

8.3.1 Modèle et schéma des données

Chaque fournisseur NGN, fédération ou entreprise peut avoir ses propres formats, schémas, définitions ou sémantiques pour représenter et échanger les données et les informations relatives aux identités. Le § 8.2.1 de [UIT-T Y.2720] décrit la nécessité d'une interopérabilité entre les systèmes de gestion IdM hétérogènes utilisant différents modèles, structures et schémas de données.

R-21 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des fonctions et des capacités permettant d'assurer l'interopérabilité entre les systèmes de gestion IdM hétérogènes qui utilisent différents modèles, structures et schémas de données selon les besoins.

8.3.2 Gestion des données d'identité

Le § 8.2 de [UIT-T Y.2720] décrit la nécessité d'une gestion des données d'identité (par exemple gestion des identificateurs, des justificatifs et des attributs). Les spécifications détaillées de gestion des données d'identité n'entre pas dans la cadre de la présente Recommandation.

Dans un réseau NGN, différentes données d'identité (par exemple des identificateurs comme une adresse de courrier électronique, des numéros de téléphone, des identificateurs URI et des adresses IP) peuvent être gérées par différents systèmes de gestion et processus d'exploitation (par exemple système d'appui à l'exploitation (OSS)/système d'appui aux activités (BSS)). Les spécifications générales suivantes sont énoncées dans le cadre de la définition d'une approche structurée et concertée concernant les interactions entre les différents systèmes de gestion et systèmes d'assistance à la clientèle nécessaires pour la prise en charge de services et de capacités de gestion IdM.

R-22 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge une interface normalisée (par exemple un portail pour les clients) pour permettre aux utilisateurs finals/abonnés d'interagir avec les systèmes et processus de gestion NGN applicables afin de faciliter les transactions des utilisateurs finals/abonnés concernant la gestion des données d'identité (par exemple modifications et mises à jour) sous réserve des réglementations et des politiques applicables en matière de protection des données.

R-23 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge les interfaces, fonctions et capacités nécessaires pour permettre d'assurer des transactions et des flux de travail cohérents entre les différents systèmes et processus de gestion liés à la gestion des données d'identité (par exemple modifications et mises à jour qui doivent passer par différents systèmes OSS/BSS, systèmes d'assistance à la clientèle et plates-formes de service d'application), selon qu'il convient, sous réserve des réglementations et des politiques applicables en matière de protection des données.

R-24 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des fonctions et des capacités permettant de journaliser et de stocker des enregistrements (par exemple des données de sauvegarde) de transactions liées à la gestion des données d'identité, sous réserve des réglementations et des politiques applicables en matière de protection des données.

R-25 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des fonctions et des capacités permettant de synchroniser les modifications et mises à jour de données d'identité entre les différents systèmes et processus de gestion, selon qu'il convient, sous réserve des réglementations et des politiques applicables en matière de protection des données.

R-26 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des fonctions et des capacités permettant de vérifier les liens entre les données d'identité associées à une entité (par exemple un abonné) et les services faisant l'objet d'un contrat (par exemple accès, voix, donnés, vidéo), sous réserve des réglementations et des politiques applicables en matière de protection des données.

8.4 Fonctions de signalisation et de commande

8.4.1 Découverte des informations d'identité

Dans un environnement NGN réparti, les informations d'identité peuvent exister dans différents éléments de réseau (par exemple serveur d'abonnement, serveur de localisation, serveur de présence, serveur d'abonnés de rattachement, etc.). Pour qu'une application puisse utiliser des informations d'identité, elle doit savoir qu'elles existent et savoir les localiser.

R-27 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des fonctions et des capacités permettant de découvrir des sources d'informations d'identité dans le domaine d'un fournisseur IdSP/NGN, par exemple, des fonctions et des capacités permettant à un serveur de gestion d'identité de découvrir l'existence d'informations d'identité dans d'autres éléments de réseau (serveurs de localisation, de présence ou d'abonnement, etc.) ou permettant à une application/un service de découvrir un serveur de gestion d'identité ou d'autres serveurs hébergeant des données d'identité.

R-28 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des fonctions et des capacités basés sur des interfaces et des protocoles normalisés permettant de découvrir des sources d'informations d'identité à travers les domaines de différents fournisseurs IdSP/NGN, par exemple, permettant de découvrir des sources d'informations d'identité dans le domaine d'un autre fournisseur IdSP/NGN conformément aux accords interréseaux applicables.

R-29 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des capacités de protection des capacités et mécanismes de découverte.

8.4.2 Contrôle d'accès aux informations d'identité

Les données d'identité ne devraient être accessibles qu'aux entités qui sont autorisées à accéder aux informations.

R-30 Il est obligatoire que les informations d'identité ne soient accessibles qu'aux entités autorisées sous réserve des réglementations et des politiques applicables. Plus précisément:

- Il est obligatoire que le fournisseur IdSP/NGN authentifie l'entité (par exemple la partie utilisatrice) demandant des données d'identité ou procède à une authentification mutuelle.
- Il est obligatoire que le fournisseur IdSP/NGN authentifie une entité (par exemple la partie utilisatrice ou la partie requérante) demandant des données d'identité, et vérifie et valide son autorisation avant que l'accès aux informations soit fourni ou que les données d'identité demandées soient échangées.

8.4.3 Communications de gestion IdM

Les systèmes et éléments de réseau doivent établir des sessions de communication pour échanger des informations d'identité (par exemple des identificateurs, des justificatifs et des attributs) situées dans différents systèmes de réseau (par exemple serveur de gestion d'identité, serveur d'abonnement, serveur de localisation, serveur de présence, etc.) qui pourraient être corrélées et vérifiées (à savoir par un serveur d'application de gestion IdM assurant des fonctions d'authentification et de corrélation) afin d'assurer des capacités de garantie d'identité.

Le fournisseur IdSP/NGN peut communiquer des assertions d'identité et des attributs associés (par exemple des déclarations et des privilèges) aux parties utilisatrices, par exemple en vue de la prise de décisions concernant le contrôle d'accès. Ainsi, les différents services d'application (appartenant à des plates-formes de fabricants différents) pourraient utiliser un service commun de gestion IdM mis à disposition au lieu de solutions indépendantes et autonomes. Les relations de communication à prendre en considération sont les suivantes:

- Intraréseau: communications à l'intérieur du domaine d'un fournisseur NGN (par exemple, entre éléments de réseau).
- Interréseaux: communications entre deux fournisseurs NGN différents.
- Fédération: communications entre des membres d'une fédération.

8.4.3.1 Communications en temps réel ou presqu'en temps réel

La solution utilisée pour découvrir et échanger des informations d'identité doit tenir compte de la question de savoir s'il est nécessaire d'avoir des communications en temps réel ou presqu'en temps réel. Cela dépendra des applications spécifiques prises en charge. Certaines applications (par exemple VoIP et TVIP) nécessiteront la validation de l'identité de l'utilisateur/abonné requérant et une autorisation pour le service d'application. D'autres applications (par exemple services de transmission de données et de messagerie) nécessiteront uniquement des sessions de communication presqu'en temps réel pour la validation de l'identité de l'utilisateur/abonné requérant et une autorisation pour le service d'application.

R-31 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des capacités d'établissement de sessions de communication permettant d'échanger des informations d'identité en temps réel ou presqu'en temps réel, selon les besoins du service d'application spécifique, notamment des sessions de communication permettant d'échanger des informations d'identité à l'intérieur du domaine d'un fournisseur NGN, entre deux fournisseurs NGN différents et entre des membres d'une fédération.

Les informations d'attribut peuvent éventuellement être limitées au statut de membre, aux fonctions liées (facturation, exploitation) et aux attributs utilisés par d'autres services (par exemple un service d'annuaire ou un service de certificat). Ainsi, la partie utilisatrice peut fournir des informations et des contenus personnalisés aux utilisateurs compte tenu de leurs attributs.

R-32 Le fournisseur IdSP/NGN et la partie utilisatrice doivent pouvoir échanger des assertions associées à une identité, notamment une assertion d'attributs.

8.4.4 Corrélation et lien

Les informations d'identité (par exemple identificateurs, justificatifs et attributs) peuvent être corrélées afin d'établir un lien et de garantir l'identité d'une entité. Ainsi, les informations d'identité associées à un abonné (par exemple l'identité d'utilisateur), à un dispositif d'abonné (par exemple l'identité de dispositif) et d'autres informations connexes comme les données d'emplacement et de profil peuvent être corrélées afin d'établir un lien et d'offrir un niveau plus élevé de garantie de l'identité de l'abonné (confiance dans la validité de l'identité).

R-33 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des capacités permettant de corréler plusieurs données relatives à l'identité (par exemple emplacement et profil) afin de pouvoir établir le lien approprié avec l'identité de l'entité, sous réserve des réglementations et des politiques applicables en matière de protection des données. Pour l'utilisation de ces capacités, le consentement spécifique et éclairé de l'utilisateur est nécessaire.

NOTE – Il est possible que la prise en charge de cette spécification soit restreinte par certaines réglementations et politiques nationales en matière de protection des données.

8.4.5 Spécifications d'authentification

L'authentification est le processus permettant d'établir la confiance dans le lien entre une identité et l'entité. L'un des moyens permettant de garantir l'authentification consiste à décrire les objectifs et les lignes directrices nécessaires pour quantifier la probabilité qu'une entité soit bien celle ou ce qu'elle prétend être. Il s'agit notamment de déterminer quels identificateurs d'entité sont plus importants que d'autres dans le processus d'identification et pourquoi certains identificateurs utilisés pour l'authentification ne devraient pas avoir la même valeur en termes d'authentification.

On trouvera dans [UIT-T Y.2702] les spécifications d'authentification dans les réseaux NGN.

Les spécifications de sécurité concernant les aspects de gestion IdM liés à l'authentification sont les suivantes:

R-34 Des entités (par exemple un utilisateur, un fournisseur IdSP/NGN, une partie utilisatrice) doivent pouvoir s'authentifier mutuellement.

R-35 Une partie utilisatrice doit pouvoir envoyer au fournisseur IdSP/NGN des demandes d'authentification d'une entité (par exemple un utilisateur/abonné).

R-36 Le fournisseur IdSP/NGN doit pouvoir assurer l'authentification d'une entité (par exemple un utilisateur/abonné) et communiquer des assertions à une partie utilisatrice.

R-37 Une partie utilisatrice doit pouvoir demander qu'une entité soit à nouveau authentifiée en spécifiant la méthode à utiliser pour cette nouvelle authentification (méthode actuelle ou autre méthode).

8.4.6 Garantie d'authentification

La garantie d'authentification est le degré de confiance obtenu dans le processus d'authentification dans le fait que le partenaire de communication est l'entité qu'il déclare être ou qu'il est censé être. La confiance repose sur le degré de confiance dans le lien entre l'entité communicante et l'identité présentée. Les entités (par exemple les utilisateurs, les services d'application, etc.) peuvent avoir des besoins différents en matière de garantie d'authentification suivant le contexte. Dans certains cas, le niveau d'authentification requis pour accéder à différentes ressources pourra varier en fonction de la sensibilité et de la valeur des informations et des transactions envisagées. Les parties utilisatrices (par exemple les utilisateurs, les fournisseurs IdSP/NGN) auront alors besoin de davantage de détails (par exemple méthodes d'authentification, nombre de facteurs d'authentification, contextes d'authentification, etc.) que d'habitude pour parvenir à la garantie d'authentification attendue. Pour cela, il faut évaluer les risques potentiels associés aux conséquences d'erreurs d'authentification ou déterminer le niveau approprié de garantie de l'identité d'une entité. Plus les erreurs

d'authentification sont susceptibles d'avoir de graves conséquences, plus les niveaux de garantie nécessaires seront élevés.

R-38 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge une ou des méthodes d'authentification appropriées suivant le ou les niveaux de garantie nécessaires.

R-39 Une partie utilisatrice doit pouvoir indiquer au fournisseur IdSP/NGN le niveau de garantie d'authentification nécessaire pour une entité.

R-40 Une négociation du niveau de garantie doit être possible entre le fournisseur IdSP/NGN, la partie utilisatrice et l'entité en cours.

8.4.6.1 Garantie d'identité et d'intégrité de dispositif d'utilisateur

Les réseaux NGN prendront en charge divers dispositifs d'utilisateur (par exemple des téléphones fixes, des combinés sans fil, des ordinateurs personnels, des PDA, des boîtiers-adaptateurs de TVIP). Les composants matériels et logiciels des dispositifs rattachés aux réseaux NGN vont des plus simples aux plus complexes. S'ils sont volés ou compromis, ils peuvent être utilisés pour orchestrer diverses attaques. Les réseaux NGN devront évidemment aussi prendre en charge des dispositifs (par exemple des terminaux non intelligents ou des téléphones ordinaires) qui ne pourront pas offrir le degré de protection nécessaire.

R-41 Un fournisseur IdSP/NGN doit pouvoir prendre en charge des dispositifs d'utilisateur final qui contiennent des capacités de sécurité et des données de gestion d'identité chiffrées (par exemple des mots de passe, des clés numériques et des certificats) dans un composant matériel inaltérable.

R-42 Un fournisseur IdSP/NGN doit pouvoir communiquer avec les capacités de sécurité intégrées dans le composant matériel inaltérable des dispositifs d'utilisateur final via des interfaces normalisées afin de prendre en charge des services d'application de sécurité reposant sur l'entité de confiance qu'est le composant matériel inaltérable spécialisé pour identifier de manière univoque et garantir l'identité des dispositifs d'utilisateur final.

Les applications qui sont exécutées sur les dispositifs d'abonné et qui permettent aux abonnés d'interagir avec des fonctionnalités de dispositif locales et des services, sont susceptibles de compromettre l'intégrité des dispositifs. Les applications Internet courantes (par exemple les navigateurs web et le courrier électronique) sont susceptibles d'introduire des vulnérabilités qui risquent d'altérer l'intégrité des dispositifs d'abonné. Les téléchargements de logiciels et de fichiers, notamment en provenance d'une source non fiable, rendent les dispositifs d'abonné vulnérables aux codes malveillants, vers, virus et chevaux de Troie. Un composant matériel inaltérable spécialisé pourrait être conçu et mis en œuvre dans les dispositifs d'utilisateur final afin de vérifier leur intégrité. Par exemple, ce composant pourrait contenir des algorithmes et des fonctions propres à un fournisseur afin de vérifier si l'intégrité a été compromise. Il pourrait inclure un modèle de référence avec un ensemble de paramètres d'intégrité bien connus afin de déterminer le code correct et de fournir des valeurs de référence pour le dispositif. Ces paramètres seraient utilisés pour comparer les valeurs réelles indiquées à la configuration et déterminer si l'unité est conforme.

R-43 Un fournisseur IdSP/NGN doit pouvoir prendre en charge des dispositifs d'utilisateur final dotés d'un composant matériel inaltérable spécialisé afin de vérifier l'intégrité des dispositifs et de confirmer cette intégrité aux applications et services.

R-44 Un fournisseur IdSP/NGN doit pouvoir communiquer avec les capacités de sécurité intégrées dans le composant matériel inaltérable des dispositifs d'utilisateur final via des interfaces normalisées afin de prendre en charge des services d'application reposant sur des vérifications d'intégrité des dispositifs et la confirmation de cette intégrité.

La perte ou le vol d'un dispositif contenant des informations PII et d'autres données sensibles peut entraîner de graves conséquences pour des particuliers, des entreprises privées ou des structures de l'Etat. Le composant matériel spécialisé conçu pour identifier de manière univoque et confirmer l'intégrité de dispositifs fiables pourrait aussi prendre en charge des capacités permettant de chiffrer et de protéger les informations PII et les autres données sensibles sur les dispositifs d'utilisateur final.

R-45 Un fournisseur IdSP/NGN doit pouvoir prendre en charge des dispositifs d'utilisateur final dotés d'un composant matériel inaltérable spécialisé afin de chiffrer et de protéger les informations PII et les autres données sensibles sur les dispositifs d'utilisateur final.

8.4.7 Prise en charge de services nécessitant un traitement prioritaire

Les systèmes et capacités de gestion IdM des réseaux NGN devront prendre en charge des services d'application et des sessions de communication nécessitant un traitement prioritaire par rapport à d'autres services. [UIT-T Y.2205] décrit les télécommunications d'urgence nécessitant un traitement spécial dans les réseaux NGN. Un exemple spécifique est le service de télécommunications d'urgence (ETS) défini dans [UIT-T E.107], qui s'appuie sur les capacités de gestion IdM utilisées pour les services ordinaires (par exemple garantie d'identité et découverte d'identités fiables). Par conséquent, les systèmes de gestion IdM doivent prendre en charge les fonctions et capacités nécessaires pour reconnaître un appel/une session ETS et lui assurer un traitement prioritaire lors de son établissement et de son maintien, compte tenu des règles et politiques nationales applicables. [UIT-T E.107] et [UIT-T Y.2205] contiennent des informations sur les services et les capacités nécessitant un traitement prioritaire.

R-46 Il est obligatoire que les systèmes de gestion IdM du fournisseur IdSP/NGN prennent en charge les fonctions et capacités nécessaires pour reconnaître un appel/une session ETS et lui assurer un traitement prioritaire lors de son établissement et de son maintien, compte tenu des règles et politiques nationales applicables.

R-47 Il est obligatoire que les éléments de réseau et les bases de données de gestion IdM utilisés pour prendre en charge les appels/sessions ETS assurent un traitement prioritaire compte tenu des règles et politiques nationales applicables. Les communications concernées sont notamment les suivantes:

- les communications de gestion IdM intraréseau (par exemple les interactions à l'intérieur du système de gestion IdM d'un fournisseur NGN);
- les communications de gestion IdM interréseaux (par exemple les interactions entre les systèmes de deux fournisseurs NGN sur la base de politiques et d'accords bilatéraux);
- les communications de gestion IdM au sein d'une fédération (par exemple les interactions entre des membres d'une fédération sur la base des règles et politiques applicables relatives aux identités fédérées).

L'Appendice III contient des exemples de cas d'utilisation liés au service ETS.

8.5 Fonctions de gestion des identités fédérées

La fédération repose sur l'établissement d'une relation entre deux entités ou plus ou sur l'établissement d'une association comprenant un nombre quelconque de fournisseurs de service et/ou de fournisseurs de service d'identité. D'une manière générale, une fédération vise à permettre à chacun de ses membres de rester indépendant tout en facilitant l'échange d'informations d'identité spécifiques pour permettre des services fédérés. Par exemple, certaines informations d'identité d'un utilisateur/abonné (par exemple un sous-ensemble du profil d'un abonné) pourraient être fédérées (c'est-à-dire mises à la disposition des membres de la fédération) dans les limites des politiques et des conditions de la fédération ainsi que des réglementations et des politiques en matière de protection des données. Grâce aux identités fédérées, la portabilité et la transmission d'informations d'identité sont possibles à travers des domaines de sécurité qui seraient autrement autonomes, dans

les limites des politiques et des conditions d'une fédération et sous réserve des règles, réglementations et politiques applicables. Grâce aux identités fédérées, les utilisateurs d'un domaine peuvent accéder en toute sécurité aux données ou systèmes d'un autre domaine sans qu'une administration de l'utilisateur complètement redondante soit nécessaire.

R-48 Il doit être possible de découvrir et d'échanger des informations relatives aux identités fédérées entre les membres d'une fédération, sous réserve des règles, réglementations et politiques applicables.

R-49 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des capacités permettant à un abonné de fournir l'autorisation nécessaire pour fédérer ses identités.

R-50 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des capacités permettant à un abonné de mettre fin à sa participation à tout ou partie des services et applications d'identité fédérée et de mettre fin à la fédération de ses identités.

R-51 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge des capacités permettant à un abonné de pouvoir fixer des permissions et des interdictions concernant les informations relatives à ses identités fédérées. Les abonnés doivent pouvoir contrôler quelles données personnelles sont données à qui et à quelle fin.

NOTE – Les spécifications de protection des informations PII énoncées au § 8.6 s'appliquent également aux identités fédérées.

D'une manière générale, chaque fournisseur NGN, entreprise ou membre de fédération peut avoir ses propres formats, schémas, définitions ou sémantique pour représenter et échanger les données et informations relatives aux identités. Ainsi, une même information, par exemple la date de naissance, peut être représentée différemment par deux systèmes différents. De même, la sémantique, les schémas, les technologies et les mécanismes utilisés pour représenter, demander et échanger des informations relatives aux identités peuvent être différents et conduire à des problèmes d'interopérabilité. Par conséquent, des capacités appropriées seront nécessaires pour permettre un relais et un interfonctionnement entre fédérations de confiance.

R-52 Il doit être possible d'assurer un relais et une interopérabilité entre fédérations de confiance qui n'utilisent pas les mêmes systèmes de gestion IdM, sémantiques, schémas, mécanismes et technologies. Ainsi, les parties utilisatrices situées dans différents domaines (par exemple domaine NGN et services web/Internet) et utilisant différentes capacités de gestion IdM et technologies doivent pouvoir interfonctionner. En particulier, la transmission sécurisée d'informations relatives aux identités fédérées doit être garantie.

8.6 Fonctions d'utilisateur/d'abonné et protection des informations PII

Les utilisateurs finals/abonnés doivent disposer d'interfaces et de capacités leur permettant de contrôler leurs informations PII et de prendre des décisions éclairées concernant leurs données personnelles. Les utilisateurs finals/abonnés devraient pouvoir exprimer leurs politiques et préférences en matière de confidentialité et négocier les conditions de divulgation des données avec le fournisseur IdSP/NGN.

Les données personnelles ne devraient être divulguées qu'aux entités autorisées sur la base des politiques applicables (par exemple consentement de l'utilisateur/abonné, réglementations publiques). De plus, la collecte, le stockage et l'utilisation d'informations PII devraient être réduits au minimum et respecter les politiques applicables.

R-53 Il est obligatoire que le fournisseur IdSP/NGN assure des service de gestion IdM et protège la confidentialité des informations PII, conformément aux réglementations, politiques et règles applicables.

R-54 Les utilisateurs finals/abonnés doivent pouvoir communiquer au fournisseur IdSP/NGN leurs préférences concernant leurs données personnelles (par exemple en matière de confidentialité) conformément aux réglementations et aux politiques applicables (par exemple déclaration de consentement des particuliers, politiques des fournisseurs, ou réglementations).

R-55 L'utilisateur final/abonné doit pouvoir vérifier l'authenticité de l'entité demandant des informations PII avant de fournir les informations demandées.

R-56 Il est obligatoire que le fournisseur IdSP/NGN supprime des informations PII lorsque les objectifs spécifiés de collecte et de conservation des données sont atteints sur la base des réglementations, des politiques et des règles applicables.

R-57 L'utilisateur final/abonné doit pouvoir agir anonymement ou sous un pseudonyme, suivant le contexte d'application et les réglementations, les politiques et les règles applicables.

8.7 Sécurité

Les informations et données d'identité sont très sensibles et sont des cibles pour les intrus. En outre, étant donné que les services et capacités de gestion IdM seront utilisés pour le contrôle d'accès aux applications des entreprises privées, des pouvoirs publics et des réseaux sociaux, les éléments de réseau et les systèmes (par exemple les éléments de réseau et les bases de données prenant en charge des fonctions et capacités de gestion IdM) seront des cibles pour les attaques et les intrusions. Par conséquent, des mesures de sécurité appropriées doivent être mises en œuvre pour sécuriser et protéger les éléments de réseau et les systèmes assurant des fonctions, services et capacités de gestion IdM.

8.7.1 Contrôle d'accès aux systèmes et aux données

Le contrôle d'accès aux systèmes repose sur des mesures de sécurité destinées à empêcher l'accès non autorisé aux éléments de réseau et aux systèmes et à leurs points d'accès associés. Il existe des menaces associées à l'accès non autorisé aux éléments de réseau et systèmes prenant en charge des fonctions, capacités et données de gestion IdM. Par conséquent, il faut établir et appliquer des mesures de contrôle d'accès appropriées afin d'empêcher l'accès non autorisé.

R-58 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge et applique des mesures de contrôle d'accès aux systèmes pour empêcher l'accès non autorisé aux éléments de réseau et aux systèmes prenant en charge des fonctions et capacités de gestion IdM. Le fournisseur IdSP/NGN ne doit autoriser une entité à accéder aux éléments de réseau et bases de données prenant en charge des fonctions et capacités de gestion IdM que si cette entité est identifiée, authentifiée et autorisée, quelle que soit l'entité (personne, processus ou système distant).

Le contrôle d'accès aux données repose sur des mesures de sécurité destinées à empêcher l'accès non autorisé aux données stockées ou approvisionnées et aux données en transit. Il existe des menaces associées à l'accès non autorisé aux données approvisionnées ou stockées relatives à la gestion IdM. Par conséquent, il faut établir et appliquer des mesures de contrôle d'accès appropriées pour empêcher l'accès non autorisé.

R-59 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge et applique des mesures de contrôle d'accès pour empêcher l'accès non autorisé aux données de gestion IdM, notamment aux données d'identité stockées ou approvisionnées dans des bases de données de gestion IdM, dans des serveurs d'application, dans un serveur d'abonnés de rattachement (HSS) ou dans tout autre élément de réseau. Le fournisseur IdSP/NGN ne doit autoriser une entité à accéder aux données de gestion IdM que si cette entité est identifiée, authentifiée et autorisée, quelle que soit l'entité (personne, processus ou système distant).

8.7.2 Intégrité des systèmes et des données

La protection de l'intégrité des éléments de réseau, systèmes et fonctions prenant en charge des services et capacités de gestion IdM doit être assurée. Il s'agit notamment des bases de données de gestion IdM et des serveurs d'application.

R-60 Il est obligatoire que le fournisseur IdSP/NGN assure la protection de l'intégrité de tous les éléments de réseau, systèmes et fonctions prenant en charge des services et capacités de gestion IdM.

La protection de l'intégrité des informations et données d'identité stockées doit être assurée afin d'empêcher toute corruption ou manipulation des données ayant une incidence sur l'intégrité.

R-61 Il est obligatoire que le fournisseur IdSP/NGN assure la protection de l'intégrité des données approvisionnées de gestion IdM.

R-62 Il est obligatoire que le fournisseur IdSP/NGN assure la protection de l'intégrité des données distribuées, communiquées, mises à jour ou modifiées, et des données hors ligne associées à la gestion IdM.

8.7.3 Confidentialité des données

R-63 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge et applique des mesures visant à protéger les données approvisionnées de gestion IdM contre les observations par des entités non autorisées (par exemple des personnes en interne non autorisées).

R-64 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge et applique des mesures visant à protéger les données de gestion IdM distribuées, communiquées, mises à jour ou modifiées, et les données hors ligne de gestion IdM contre les observations par des entités non autorisées (par exemple des personnes en interne non autorisées).

8.7.4 Protection de la sécurité des communications de gestion IdM

Les communications de gestion IdM (signalisation et média) doivent être protégées contre l'accès non autorisé, la corruption, la manipulation et l'interception (par exemple écoute clandestine).

R-65 Il est obligatoire que le fournisseur IdSP/NGN assure la protection de l'intégrité et de la confidentialité des communications de gestion IdM intraréseau et interréseaux. La protection de l'intégrité de l'ensemble du trafic de signalisation et de média lié à la gestion IdM traversant une interface réseau-réseau (NNI), une interface application-réseau (ANI) ou une interface serveur-réseau (SNI) entre domaines de réseau doit être assurée.

8.7.5 Sécurité de la gestion

L'accès aux fins de gestion aux éléments de réseau NGN et aux données configurées doit être sécurisé et protégé contre l'accès et les contrôles non autorisés.

R-66 Il est obligatoire que le fournisseur IdSP/NGN empêche l'accès non autorisé aux interfaces de gestion et les contrôles non autorisés des éléments de réseau et des entités fonctionnelles prenant en charge la gestion IdM.

Le trafic de gestion doit être sécurisé et protégé contre la corruption, la manipulation et l'observation non autorisée.

R-67 Il est obligatoire que le fournisseur IdSP/NGN assure la protection de l'intégrité et de la confidentialité du trafic de gestion associé à la prise en charge de la gestion IdM.

8.7.6 Journalisation de sécurité et d'audit

Il est nécessaire de générer des journaux de sécurité et d'audit dans lesquels seront enregistrés des événements afin de faciliter les investigations ultérieures concernant des activités spécifiques.

R-68 Il est obligatoire que le fournisseur IdSP/NGN génère des journaux de sécurité dans lesquels seront enregistrés des événements afin de faciliter les investigations ultérieures concernant des activités spécifiques (par exemple connexions, modification de ressources et de données de système essentielles, accès aux fins de gestion aux paramètres et ressources NGN configurés) en lien avec la prise en charge de la gestion IdM.

8.7.7 Protection contre les attaques par déni de service (DoS) et par déni de service réparti (DDoS)

Une grande disponibilité des services et capacités de gestion IdM est nécessaire. Il faut donc les protéger contre les menaces DoS et DDoS susceptibles d'affecter la disponibilité.

R-69 Il est obligatoire que le fournisseur IdSP/NGN assure une protection contre les attaques DoS, DDoS et les autres types d'attaques qui ont une incidence sur la disponibilité des services et capacités de gestion IdM. Il s'agit notamment de prendre en charge et d'utiliser des capacités et outils appropriés pour détecter et isoler les attaques DoS et DDoS et les autres types d'attaques et pour en réduire les effets.

8.7.8 Surveillance et détection des intrusions

R-70 Il est obligatoire que le fournisseur IdSP/NGN prenne en charge et utilise des outils appropriés de surveillance de la sécurité et de détection des intrusions afin de détecter les fraudes, les abus et les intrusions dans les éléments de réseau et les systèmes de gestion IdM.

Appendice I

Cas d'utilisation généraux de la gestion IdM

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

I.1 Introduction

Le présent appendice décrit des cas d'utilisation généraux de la gestion IdM par les Etats, les entreprises privées et les utilisateurs finals/abonnés.

I.2 Etats

Les Etats peuvent utiliser des capacités de gestion IdM pour améliorer ou prendre en charge des applications et des transactions entre les structures de l'Etat et les citoyens, entre différents organismes publics (services administratifs fédérés) et entre différents Etats (par exemple des services fédérés entre Etats). Comme exemples de cas d'utilisation, on peut citer:

- La garantie d'identification des citoyens: les Etats peuvent utiliser la gestion IdM pour valider l'identité des citoyens souhaitant bénéficier de services administratifs en ligne tout en améliorant la protection des informations PII. Dans le cas des soins de santé par exemple, la sensibilité des informations relatives à la santé souligne l'importance de réduire les données au minimum et, plus généralement, la nécessité d'assurer la sécurité et la confidentialité des informations d'identité.
- La garantie d'identification des fonctionnaires pour les services administratifs fédérés: les structures de l'Etat peuvent utiliser des capacités de gestion IdM pour élaborer des solutions communes d'identification fiable et sécurisée des fonctionnaires qui offrent une meilleure sécurité, une certaine efficacité, une réduction des fraudes liées à l'identité et la protection de la vie privées.
- L'amélioration ou la prise en charge de services fédérés entre différents Etats: la gestion IdM peut être utilisée pour améliorer ou prendre en charge des services fédérés entre différents Etats. Par exemple, des Etats peuvent collaborer pour élaborer à l'intention des citoyens voyageant d'un pays à un autre des solutions améliorées de gestion IdM qui tiennent compte de la sécurité, de la confidentialité et de l'expérience des utilisateurs.

I.3 Entreprise privée

La gestion IdM peut être utilisée pour aider les entreprises privées à améliorer ou prendre en charge des activités nouvelles ou existantes tout en améliorant la sécurité, la confidentialité et la protection des informations PII. Comme exemples de cas d'utilisation, on peut citer:

- Les services d'identité fédérée: la gestion IdM peut être utilisée pour prendre en charge des services d'authentification et de déconnexion uniques parmi plusieurs partenaires commerciaux (fournisseurs NGN, fournisseurs de services web, fournisseurs de contenus et fournisseurs tiers).
- Les services de communication: la gestion IdM peut être utilisée par les fournisseurs NGN pour permettre aux utilisateurs finals/abonnés de bénéficier de services d'application sur différentes plates-formes (par exemple réseaux IP gérés, plates-formes Internet et mobile) et pour permettre aux utilisateurs d'accéder aux applications qu'ils ont choisies sur plusieurs plates-formes par des moyens adaptés à leurs propres préférences.
- Les applications et transactions financières électroniques: la gestion IdM peut être utilisée pour améliorer ou prendre en charge des applications de paiement électronique pour les transactions de commerce électronique.

I.4 Utilisateurs finals/abonnés

Pour les utilisateurs finals/abonnés, la gestion IdM peut être utilisée pour améliorer l'expérience et le contrôle des informations PII. Comme exemples de cas d'utilisation, on peut citer:

- Le contrôle par les utilisateurs des informations PII: la gestion IdM peut être utilisée pour améliorer l'expérience des utilisateurs pour permettre de contrôler les informations PII. Les particuliers peuvent utiliser plusieurs pseudonymes pour participer à différentes activités (par exemple vérification des fils d'actualité, publication de messages sur des blogs, gestion des réseaux sociaux et échange de photos ou de musique). La gestion IdM peut permettre d'offrir aux particuliers davantage de possibilités quant à leur participation à différentes communautés et quant à la mesure dans laquelle ils souhaitent que des aspects de leurs différentes identités soient reliés (contrôle de leurs informations PII).
- Les réseaux sociaux: la gestion IdM peut être utilisée pour améliorer ou prendre en charge des applications de réseaux sociaux en fournissant les outils nécessaires pour permettre aux utilisateurs de contrôler efficacement les informations PII et la responsabilité.

Appendice II

Cas d'utilisation de la gestion IdM pour les applications NGN

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

II.1 Introduction

Le présent appendice donne des exemples de cas d'utilisation de la gestion d'identité (IdM) pour les réseaux NGN, qui ont servi de base à l'élaboration des spécifications de gestion IdM pour les réseaux NGN.

II.2 Exemple de base de cas d'utilisation

La Figure II.1 montre un exemple de base de cas d'utilisation avec trois éléments de base. Les autres scénarios possibles (par exemple des scénarios centrés sur l'utilisateur) sont décrits à l'Appendice V.

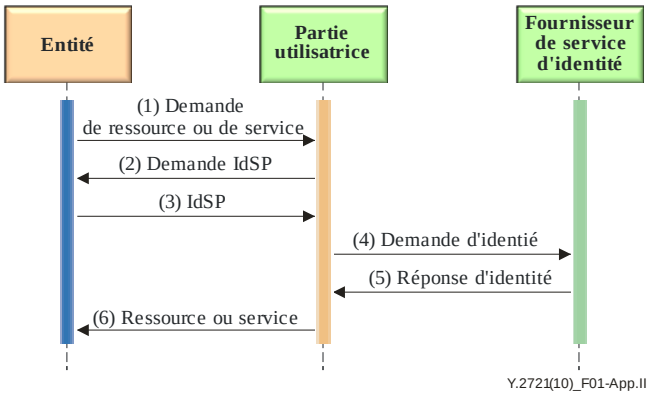


Figure II.1 – Exemple de base de cas d'utilisation

Les trois éléments sont une entité (une partie assertante ou une entité principale) qui demande des services à une partie utilisatrice (qui peut être un réseau ou une application) et qui obtient une assertion d'identité associée (assertion anonyme ou pseudonyme) auprès d'un fournisseur de service d'identité (IdSP) sur la base d'une politique de confiance et de sécurité.

Le flux d'informations de gestion IdM de haut niveau représenté sur la Figure II.1 est le suivant.

1) L'entité fournit une identité déclarée à la partie utilisatrice (le fournisseur de ressources ou de services) et demande une ressource ou un service à cette partie utilisatrice.

2) La partie utilisatrice (réseau ou application) a besoin que l'entité soit authentifiée avant de fournir la ressource ou le service demandé. Pour l'authentification, la partie utilisatrice a besoin d'obtenir des informations auprès du fournisseur IdSP approprié, qui doit être déterminé et contacté. La partie utilisatrice retourne une "demande d'info IdSP" à l'entité, lui demandant de fournir le nom du fournisseur IdSP approprié.

3) L'entité répond à cette "demande d'info IdSP" en donnant l'identification du fournisseur IdSP approprié à la partie utilisatrice. Elle peut donner l'identification de plusieurs fournisseurs IdSP.

4) La partie utilisatrice demande à son tour au ou aux fournisseurs IdSP appropriés de valider l'identité déclarée de l'entité avec un niveau de confiance suffisant (niveau de garantie), comme demandé.

5) Le fournisseur IdSP confirme l'identité déclarée de l'entité. Parmi les fonctions du fournisseur IdSP peut figurer la délégation (ce qui signifie que le fournisseur IdSP peut déléguer certains aspects du processus d'authentification à d'autres fournisseurs IdSP et

pour cela, leur relayer l'assertion d'identité). La partie utilisatrice peut ensuite adresser d'autres demandes au ou aux fournisseurs IdSP, au cas où une authentification avec un niveau de garantie plus élevé serait nécessaire, ou pour d'autres capacités propres à la mise en œuvre.

6) Après avoir reçu du ou des fournisseurs IdSP la validation de l'identité déclarée de l'entité, la partie utilisatrice fournit la ressource ou le service demandé.

Des combinaisons de ces trois éléments (entité, partie utilisatrice et fournisseur IdSP) sont possibles. Peu importent les supports sous-jacents, pourvu que les mécanismes de communication soient "bien structurés" avec des syntaxes et des profils qui sont connus ou qui sont susceptibles de pouvoir être obtenus par les parties impliquées, si celles-ci possèdent les permissions nécessaires pour utiliser les mécanismes. Le cas échéant, il convient d'utiliser des mécanismes normalisés pour assurer une interopérabilité fiable et globale.

Par ailleurs, d'autres flux d'informations de gestion IdM de haut niveau sont possibles. Par exemple:

1) La partie utilisatrice peut demander des justificatifs d'authentification directement auprès de l'entité.

2) L'entité peut fournir ses justificatifs d'authentification à un fournisseur IdSP de confiance.

3) Le fournisseur IdSP peut valider les justificatifs fournis par l'entité puis générer de nouveaux justificatifs pour l'entité, afin de répondre à la demande d'authentification de la partie utilisatrice.

4) L'entité (ou son délégué) peut obtenir les justificatifs générés par le fournisseur IdSP et les donner à la partie utilisatrice.

5) Les justificatifs générés envoyés par l'entité à la partie utilisatrice peuvent contenir soit 1) une copie des déclarations d'identité générées par le fournisseur IdSP; soit 2) une référence à ces déclarations.

De plus, l'entité peut décider de ne pas donner les justificatifs d'authentification générés par le fournisseur IdSP à la partie utilisatrice.

Il est également possible d'avoir une hiérarchie de fournisseurs d'identité ou une hiérarchie de parties utilisatrices. Il est également possible qu'une entité ait plusieurs délégués.

II.3 Utilisation de systèmes communs de gestion IdM pour prendre en charge plusieurs services d'application (par exemple téléphonie, données, TVIP) à l'intérieur du réseau d'un fournisseur de service

II.3.1 Aperçu

En principe, les fournisseurs de réseau/service (par exemple les fournisseurs NGN) prendront en charge et hébergeront plusieurs applications et services. Les réseaux NGN étant répartis, différents services d'application peuvent être hébergés sur différents éléments de réseau et différentes plates-formes propres à un fournisseur (par exemple VoIP, données et TVIP). Les différents services peuvent avoir différents moyens de contrôle d'accès propres à un fournisseur ou propres à une technologie qui ne sont pas nécessairement compatibles entre eux et qui devront donc être configurés, gérés et utilisés séparément.

Une approche dans laquelle une infrastructure commune de gestion IdM permet d'assurer plusieurs applications/services peut être avantageuse sur le plan des coûts et de l'efficacité des activités. Elle pourrait aussi service d'approche standard permettant aux développeurs d'applications d'utiliser des éléments communs pour la gestion IdM plutôt que chaque application/service prenne en charge des fonctions de gestion IdM spécifiques (par exemple des capacités et mécanismes de contrôle d'accès propres à un fournisseur) et permettant d'avoir un processus efficace pour concevoir, mettre en œuvre et offrir des services d'application. De plus, une approche commune peut faciliter la gestion

des risques de sécurité pour chaque service d'application et pour l'infrastructure de réseau dans son ensemble.

Les solutions de gestion IdM pour les réseaux NGN incluraient à la fois des solutions intraréseau (c'est-à-dire des solutions à l'intérieur du domaine d'un fournisseur NGN) et des solutions interréseaux (c'est-à-dire des solutions entre différents fournisseurs NGN y compris des fournisseurs tiers). Les solutions intraréseau peuvent notamment permettre des interactions entre les différents éléments de réseau ou composants à l'intérieur du domaine d'un fournisseur NGN pour la gestion IdM (par exemple les déclarants, les systèmes utilisateurs et les systèmes d'identité). Les solutions interréseaux peuvent notamment permettre des interactions entre les éléments de réseau à travers différents domaines NGN pour la gestion IdM (par exemple les déclarants, les parties utilisatrices et les fournisseurs IdSP).

NOTE – Un fournisseur NGN peut aussi être un fournisseur IdSP.

II.3.2 Description du cas d'utilisation

Cet exemple de cas d'utilisation illustre comment plusieurs services d'application (par exemple VoIP, données et TVIP) utilisent une infrastructure commune de gestion d'identité pour le contrôle d'accès et la protection de la sécurité. Dans ce cas d'utilisation, des interactions existent entre les entités suivantes:

- utilisateur final (utilisateur final et/ou dispositif d'utilisateur final);
- système utilisateur (service d'application ou système de réseau);
- système de gestion IdM (système de réseau fournissant des services de gestion IdM tels que l'enregistrement, l'authentification et l'autorisation, et des informations relatives au profil d'abonnement).

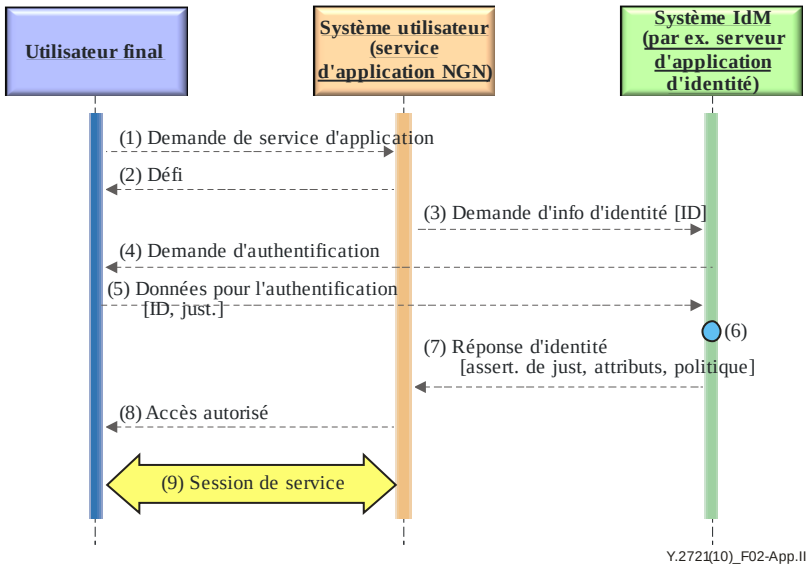


Figure II.2 – Exemple de base du cas d'utilisation

La Figure II.2 illustre un exemple de base dans lequel un service d'application utilise les services d'un système de gestion IdM externe ou indépendant par rapport au service d'application pour le contrôle d'accès et la gestion des privilèges. Les flux d'appel sont les suivants:

1) Demande de service d'application: ce flux d'informations représente l'invocation du service d'application par l'utilisateur final.

2) Défi: le service d'application envoie en réponse un défi pour l'accès de l'utilisateur.

3) Demande d'informations d'identité [ID d'utilisateur]: le service d'application envoie une demande au système de gestion IdM en vue de l'assertion de l'identité de l'utilisateur et de la fourniture d'attributs associés à l'identité de l'utilisateur, qui peuvent notamment inclure des informations comme le profil de service, les privilèges, les préférences et des informations relatives aux politiques, par exemple toute politique ou restriction associée à l'identité.

4) Demande d'authentification: le système de gestion IdM envoie à l'utilisateur une demande d'authentification.

5) Données pour l'authentification [justificatifs]: l'utilisateur fournit des informations pour l'authentification (par exemple identité de l'utilisateur et mot de passe ou numéro d'identification personnel).

6) Authentification: le système de gestion IdM procède à l'authentification et obtient les autres informations nécessaires, par exemple des informations provenant d'autres systèmes de réseau (serveur HSS par exemple).

7) Réponse d'informations d'identité [assertions de justificatifs, attributs, politique]: le système de gestion IdM fournit des informations assertant les justificatifs. Parmi les autres informations pouvant être incluses, on peut citer les attributs associés à l'identité de l'utilisateur (par exemple privilèges et préférences) et la politique associée aux informations d'identité (par exemple toute restriction concernant l'utilisation, l'affichage et la diffusion).

8) Autorisation d'accès: le service d'application indique à l'utilisateur que l'accès au service est autorisé.

9) Session de service d'application: ce flux d'informations représente la session établie avec succès entre l'utilisateur et le service d'application.

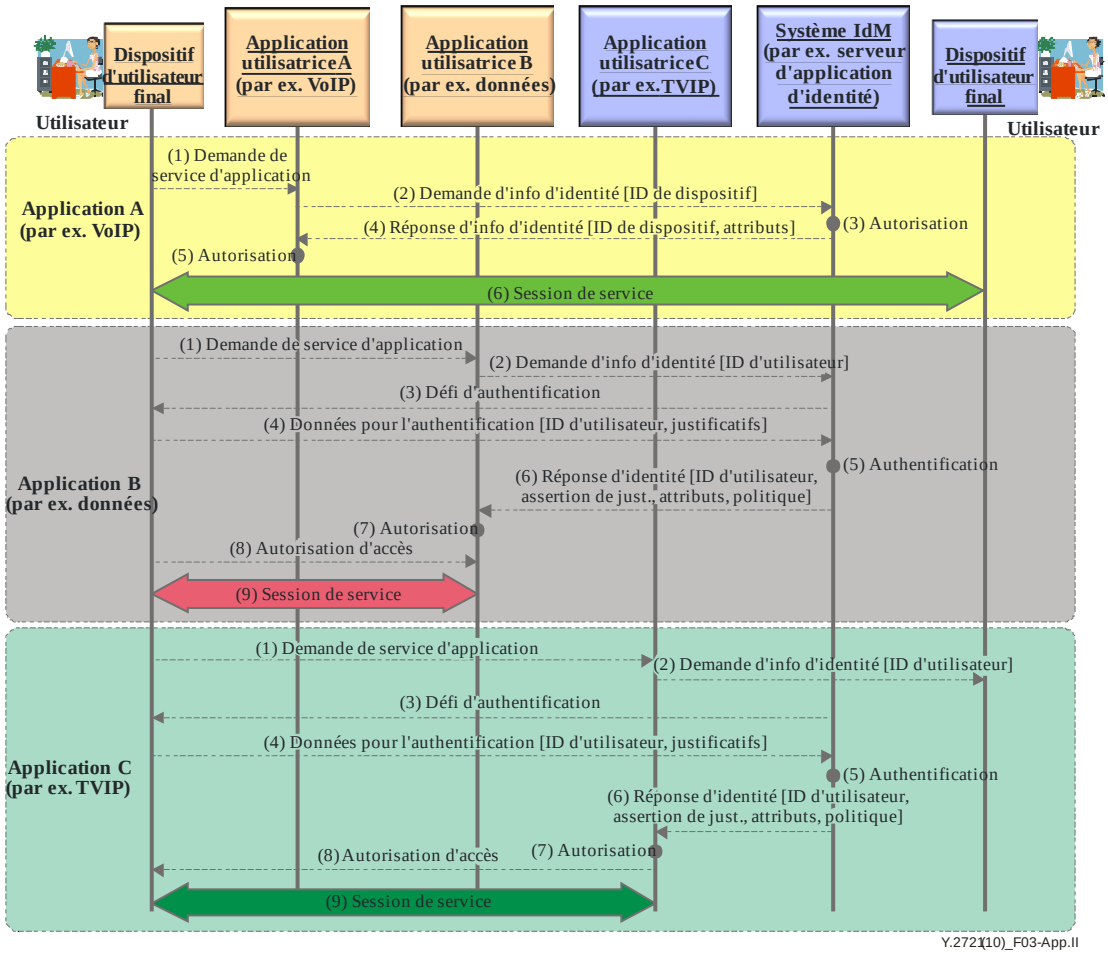


Figure II.3 – Utilisation d'une infrastructure commune de gestion IdM par plusieurs services d'application

La Figure II.3 montre un exemple de cas d'utilisation dans lequel plusieurs services d'application (par exemple VoIP, données et TVIP) utilisent un système commun de gestion IdM externe et indépendant par rapport aux services d'application. Dans cet exemple, on suppose que l'enregistrement du dispositif d'utilisateur final et son rattachement au fournisseur de service se font selon les procédures normales.

Les flux pour l'application A (VoIP) sont les suivants:

1) Demande de service d'application: ce flux d'informations représente le lancement d'un appel par l'utilisateur final.

2) Demande d'informations d'identité [ID de dispositif]: le service d'application demande au système de gestion IdM de vérifier si le dispositif d'utilisateur final est autorisé à utiliser le service de VoIP. Dans cet exemple, on suppose que le service de VoIP est basé sur le profil d'abonnement du dispositif d'utilisateur ou de la ligne (par exemple abonnement xDSL).

3) Autorisation: le système de gestion IdM détermine si l'utilisateur final est autorisé à utiliser le service de VoIP.

   NOTE 1 – On suppose que pour cela, il faut récupérer les informations de profil d'abonnement du dispositif d'utilisateur final ou de la ligne (par exemple xDSL). On suppose aussi que pour la VoIP, l'authentification de l'utilisateur final n'est pas nécessaire.

4) Réponse d'informations d'identité [ID de dispositif, attributs]: le système de gestion IdM fournit des attributs associés à l'ID de dispositif (c'est-à-dire indique si le dispositif est autorisé à utiliser le service de VoIP), notamment des informations pertinentes obtenues à partir du profil d'abonnement (privilèges et préférences par exemple).

5) Autorisation d'accès: le service d'application indique à l'utilisateur que l'accès au service est autorisé.

6) Session de service d'application: ce flux d'informations représente la session d'appel établie avec succès entre les utilisateurs.

Les flux d'appel pour l'application B (données) sont les suivants:

1) Demande de service d'application: ce flux d'informations représente l'invocation du service d'application par l'utilisateur final.

2) Demande d'informations d'identité [ID d'utilisateur]: le service d'application envoie une demande au système de gestion IdM en vue de l'assertion de l'identité de l'utilisateur et de la fourniture d'attributs associés à l'identité de l'utilisateur, qui peuvent notamment inclure des informations comme le profil de service, les privilèges, les préférences et des informations relatives aux politiques, par exemple toute politique ou restriction associée à l'identité.

3) Défi d'authentification: le système de gestion IdM envoie à l'utilisateur une demande d'authentification.

4) Données pour l'authentification [justificatifs]: l'utilisateur fournit des informations pour l'authentification (par exemple identité d'utilisateur et mot de passe ou numéro d'identification personnel).

5) Authentification: le système de gestion IdM procède à l'authentification et obtient les autres informations nécessaires, par exemple des informations provenant d'autres systèmes de réseau (serveur HSS ou autre base de données d'abonnement par exemple).

6) Réponse d'informations d'identité [assertions de justificatifs, attributs, politique]: le système de gestion IdM fournit des informations assertant les justificatifs. Parmi les autres informations pouvant être incluses, on peut citer les attributs associés à l'identité de l'utilisateur (par exemple privilèges et préférences) et la politique associée aux informations d'identité (par exemple toute restriction concernant l'utilisation, l'affichage et la diffusion).

7) Autorisation: après avoir traité les informations, le service d'application détermine que l'utilisateur est autorisé à utiliser le service.

8) Autorisation d'accès: le service d'application indique à l'utilisateur que l'accès au service est autorisé.

9) Session de service d'application: ce flux d'informations représente la session établie avec succès entre l'utilisateur et le service d'application.

Les flux d'appel pour l'application C (TVIP) sont les suivants:

1) Demande de service d'application: ce flux d'informations représente l'invocation du service d'application par l'utilisateur final.

2) Demande d'informations d'identité [ID d'utilisateur]: le service d'application envoie une demande au système de gestion IdM en vue de l'assertion de l'identité de l'utilisateur et de la fourniture d'attributs associés à l'identité de l'utilisateur, qui peuvent notamment inclure des informations comme le profil de service, les privilèges, les préférences et des informations relatives aux politiques, par exemple toute politique ou restriction associée à l'identité.

3) Défi d'authentification: le système de gestion IdM envoie à l'utilisateur une demande d'authentification.

4) Données pour l'authentification [justificatifs]: l'utilisateur fournit des informations pour l'authentification (par exemple identité d'utilisateur et mot de passe ou numéro d'identification personnel).

5) Authentification: le système de gestion IdM procède à l'authentification et obtient les autres informations nécessaires, par exemple des informations provenant d'autres systèmes de réseau (serveur HSS ou autre base de données d'abonnement par exemple).

6) Réponse d'informations d'identité [assertions de justificatifs, attributs, politique]: le système de gestion IdM fournit des informations assertant les justificatifs. Parmi les autres informations pouvant être incluses, on peut citer les attributs associés à l'identité de l'utilisateur (par exemple privilèges et préférences) et la politique associée aux informations d'identité (par exemple toute restriction concernant l'utilisation, l'affichage et la diffusion).

7) Autorisation: après avoir traité les informations, le service d'application détermine que l'utilisateur est autorisé à utiliser le service.

8) Autorisation d'accès: le service d'application indique à l'utilisateur que l'accès au service est autorisé.

9) Session de service d'application: ce flux d'informations représente la session établie avec succès entre l'utilisateur et le service d'application.

NOTE 2 – Pour assurer l'authentification mutuelle (c'est-à-dire pour authentifier le fournisseur d'application ou de service), d'autres fonctionnalités et flux seront nécessaires. Ils ne sont toutefois pas représentés sur la Figure II.3.

II.3.3 Conséquences

Les exigences découlant de cet exemple de cas d'utilisation sont les suivantes:

- Une solution commune de gestion IdM peut être mise en œuvre dans le réseau NGN et être utilisée par plusieurs services d'application indépendamment de la plate-forme d'application ou de la solution du fournisseur.
- Les fonctions communes de gestion IdM ne doivent pas être utilisées si elles sont contraires aux principes de limitation de la collecte de données, de minimalisation des données, de séparation des données, de spécification de la finalité et de limitation de l'utilisation.
- Le réseau NGN doit prendre en charge une approche normalisée et structurée pour permettre aux services d'application de découvrir le ou les systèmes de gestion IdM et d'échanger des données d'identité en toute sécurité.

II.4 Authentification unique/déconnexion unique pour plusieurs services d'application (par exemple téléphonie, données et TVIP) à l'intérieur du réseau d'un fournisseur de service

II.4.1 Aperçu

Les utilisateurs doivent généralement s'authentifier auprès de plusieurs systèmes hébergeant des services d'application (par exemple VoIP, données et TVIP), ce qui nécessite un nombre équivalent de dialogues d'authentification, dans chacun desquels les noms d'utilisateur et les informations d'authentification nécessaires peuvent être différents. Les administrateurs de système doivent gérer de façon coordonnée les comptes d'utilisateur dans chacun des multiples systèmes accessibles afin de maintenir l'intégrité de l'application de la politique de sécurité.

Les utilisateurs finals/abonnés souhaitent des fonctionnalités faciles à utiliser du type "authentification/déconnexion uniques". Le principe de l'"authentification unique" est qu'un utilisateur final, un dispositif ou une combinaison utilisateur final et dispositif peut, grâce à une seule authentification (en fournissant des données de justificatifs pour l'authentification et l'autorisation) pour un service dans un réseau de prochaine génération (NGN), être ensuite authentifié pour un ou plusieurs autres services dans le même réseau NGN (autrement dit l'utilisateur final n'a pas à s'authentifier pour chaque service). Le terme "authentification" employé ici correspond aux termes anglais "sign-on", "register with", "log-on" ou "log-in". De même, la

"déconnexion unique" permet d'éviter d'avoir à se déconnecter de chaque service d'application dans une session donnée.

Les services d'authentification/déconnexion uniques présentent notamment les avantages suivants:

- Réduction du temps passé par les utilisateurs dans les opérations d'authentification auprès de différents domaines, et réduction des risques d'échec des opérations d'authentification.
- Amélioration de la sécurité du fait que l'utilisateur a besoin de traiter et de mémoriser un moins grand nombre d'informations d'authentification.
- Réduction du temps passé par les administrateurs de système à ajouter et supprimer des utilisateurs dans le système ou à modifier leurs droits d'accès et amélioration de la réponse fournie par lesdits administrateurs.
- Amélioration de la sécurité du fait que les administrateurs de système sont davantage en mesure de maintenir l'intégrité de la configuration des comptes d'utilisateur et notamment en mesure d'interdire ou de supprimer l'accès d'un utilisateur individuel à toutes les ressources du système de manière coordonnée et cohérente.

II.4.2 Description du cas d'utilisation

Cet exemple de cas d'utilisation illustre l'utilisation d'un système de gestion IdM pour la prise en charge de l'"authentification unique/déconnexion unique" pour plusieurs services d'application (par exemple VoIP, données et TVIP) à l'intérieur du domaine d'un fournisseur NGN. Dans ce cas d'utilisation, des interactions existent entre les entités suivantes:

- Utilisateur final (utilisateur final et/ou dispositif d'utilisateur final).
- Système utilisateur (service d'application ou système de réseau).
- Système de gestion IdM (système de réseau fournissant des services de gestion IdM tels que l'enregistrement, l'authentification et l'autorisation, et des informations relatives au profil d'abonnement).

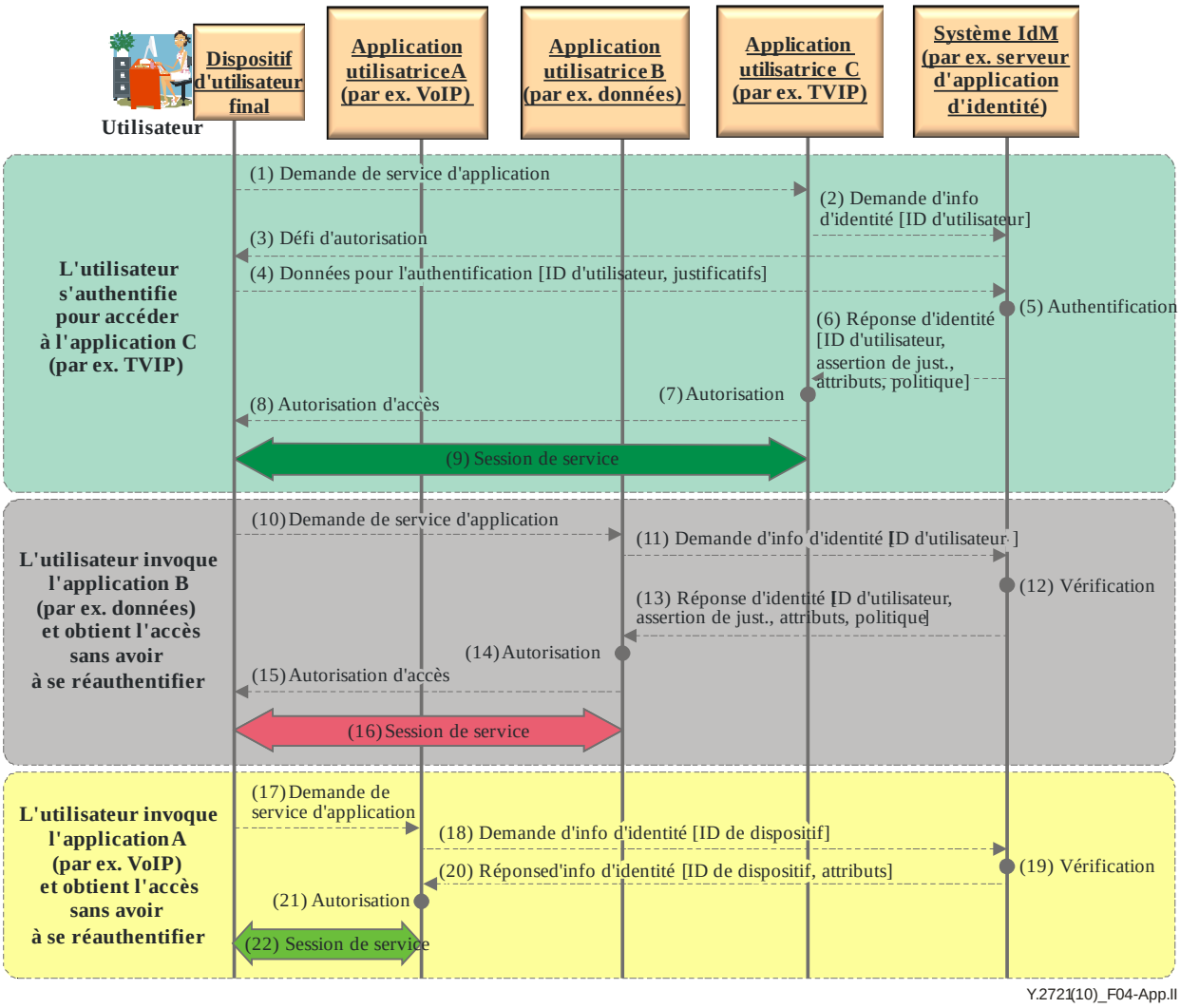


Figure II.4 – Service d'authentification unique

La Figure II.4 illustre le cas d'un utilisateur final/abonné qui utilise un service d'authentification unique pour accéder à plusieurs services d'application (par exemple VoIP, données et TVIP). Dans cet exemple, on suppose que l'enregistrement du dispositif d'utilisateur final et son rattachement au réseau NGN se font selon les procédures normales.

Les flux d'appel sont les suivants:

1) Demande de service d'application: ce flux d'informations représente l'invocation du service d'application C (TVIP) par l'utilisateur final.

2) Demande d'informations d'identité [ID d'utilisateur]: le service d'application C (TVIP) envoie une demande au système de gestion IdM en vue de l'assertion de l'identité de l'utilisateur et de la fourniture d'attributs associés à l'identité de l'utilisateur, qui peuvent notamment inclure des informations comme le profil de service, les privilèges, les préférences et des informations relatives aux politiques, par exemple toute politique ou restriction associée à l'identité.

3) Défi d'authentification: le système de gestion IdM envoie à l'utilisateur un défi d'authentification.

4) Données pour l'authentification [justificatifs]: l'utilisateur fournit des informations pour l'authentification (par exemple identité d'utilisateur et mot de passe ou numéro d'identification personnel).

5) Authentification: le système de gestion IdM procède à l'authentification et obtient les autres informations nécessaires, par exemple des informations provenant d'autres systèmes de réseau (serveur HSS ou autre base de données d'abonnement par exemple).

6) Réponse d'informations d'identité [assertions de justificatifs, attributs, politique]: le système de gestion IdM fournit des informations assertant les justificatifs. Parmi les autres informations pouvant être incluses, on peut citer les attributs associés à l'identité de l'utilisateur (par exemple privilèges et préférences) et la politique associée aux informations d'identité (par exemple toute restriction concernant l'utilisation, l'affichage et la diffusion).

7) Autorisation: après avoir traité les informations, le service d'application C (TVIP) détermine que l'utilisateur est autorisé à utiliser le service.

8) Autorisation d'accès: le service d'application C (TVIP) indique à l'utilisateur que l'accès au service est autorisé.

9) Session de service d'application: ce flux d'informations représente la session établie avec succès entre l'utilisateur et le service d'application C (TVIP).

10) Demande de service d'application: ce flux d'informations représente l'invocation du service d'application B (données) par l'utilisateur final.

11) Demande d'informations d'identité [ID d'utilisateur]: le service d'application B (données) envoie une demande au système de gestion IdM en vue de l'assertion de l'identité de l'utilisateur et de la fourniture d'attributs associés à l'identité de l'utilisateur, qui peuvent notamment inclure des informations comme le profil de service, les privilèges, les préférences et des informations relatives aux politiques, par exemple toute politique ou restriction associée à l'identité.

12) Vérification: le système de gestion IdM traite la demande, détermine que l'authentification unique s'applique et vérifie que l'authentification de l'utilisateur est toujours valable.

13) Réponse d'informations d'identité [assertions de justificatifs, attributs, politique]: le système de gestion IdM fournit des informations assertant les justificatifs. Parmi les autres informations pouvant être incluses, on peut citer les attributs associés à l'identité de l'utilisateur (par exemple privilèges et préférences) et la politique associée aux informations d'identité (par exemple toute restriction concernant l'utilisation, l'affichage et la diffusion).

14) Autorisation: après avoir traité les informations, le service d'application B (données) détermine que l'utilisateur est autorisé à utiliser le service.

15) Autorisation d'accès: le service d'application B (données) indique à l'utilisateur que l'accès au service est autorisé.

16) Session de service d'application: ce flux d'informations représente la session établie avec succès entre l'utilisateur et le service d'application B (données).

17) Demande de service d'application: ce flux d'informations représente l'invocation du service d'application A (VoIP) par l'utilisateur final.

18) Demande d'informations d'identité [ID de dispositif]: le service d'application A (VoIP) envoie une demande au système de gestion IdM en vue de l'assertion de l'identité de l'utilisateur et de la fourniture d'attributs associés à l'identité du dispositif.

19) Vérification: le système de gestion IdM traite la demande, détermine que l'authentification unique s'applique et vérifie que l'authentification de l'utilisateur est toujours valable.

20) Réponse d'informations d'identité [assertions de justificatifs, attributs, politique]: le système de gestion IdM fournit des informations assertant les justificatifs. Parmi les autres informations pouvant être incluses, on peut citer les attributs associés à l'identité du dispositif (par exemple privilèges et préférences) et la politique associée aux informations d'identité (par exemple toute restriction concernant l'utilisation, l'affichage et la diffusion).

21) Autorisation: après avoir traité les informations, le service d'application A (VoIP) détermine que l'utilisateur est autorisé à utiliser le service.

22) Session de service d'application: ce flux d'informations représente la session établie avec succès entre l'utilisateur et le service d'application A (VoIP).

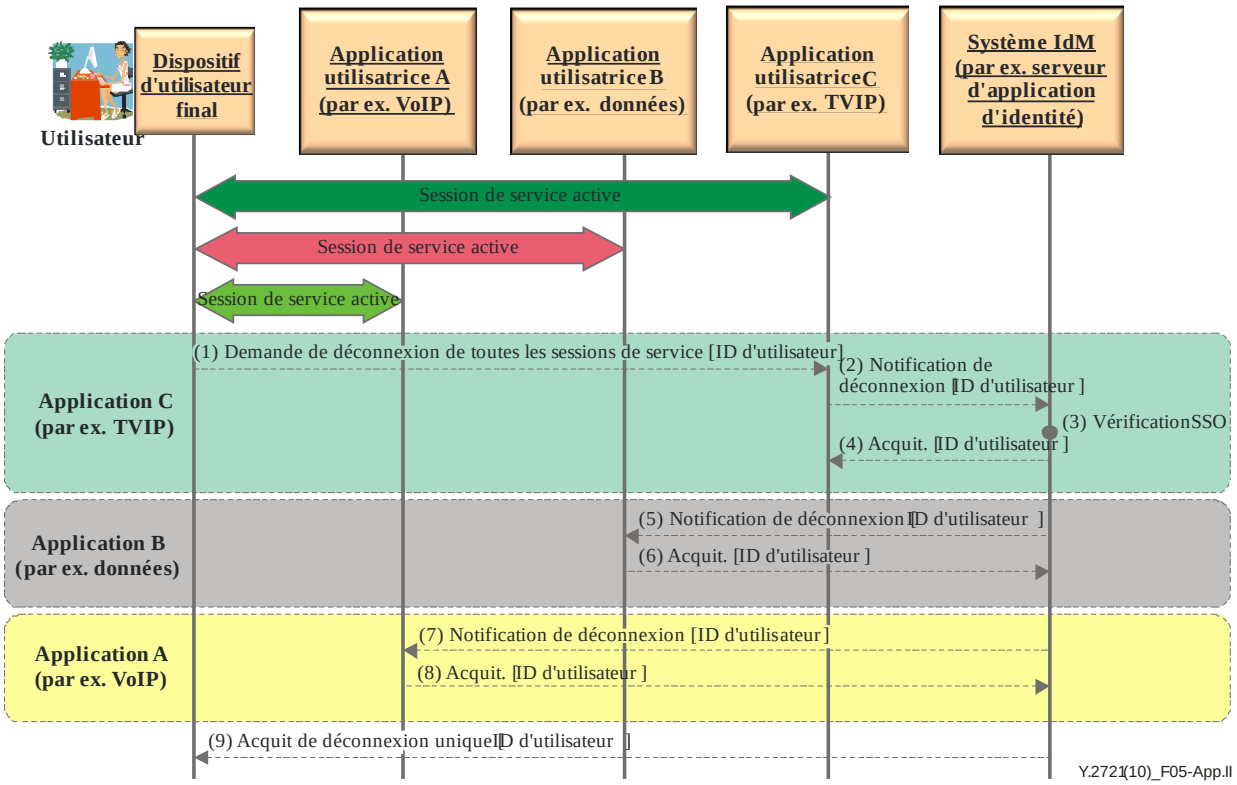


Figure II.5 – Service de déconnexion unique

La Figure II.5 illustre le cas d'un service de "déconnexion unique" permettant à l'utilisateur de se déconnecter automatiquement de plusieurs services d'application (VoIP, données et TVIP) sans avoir à se déconnecter de chaque service d'application dans la session. Dans ce cas d'utilisation, on suppose que l'utilisateur est dans une session de service avec les services d'application actifs A (VoIP), B (données) et C (TVIP).

Les flux d'appel sont les suivants:

1) Déconnexion de service [ID d'utilisateur]: ce flux d'appel représente la demande de l'utilisateur de mettre fin à toutes les sessions de service.

2) Notification de déconnexion [ID d'utilisateur]: le service d'application C (TVIP) informe le système de gestion IdM de la demande de déconnexion de l'utilisateur.

3) Vérification SSO: le système de gestion IdM détermine que la déconnexion unique s'applique et vérifie les services d'application actifs.

4) Acquittement [ID d'utilisateur]: le système de gestion IdM envoie un acquittement de fin de session de service au service d'application C (TVIP).

5) Notification de déconnexion [ID d'utilisateur]: le système de gestion IdM informe le service d'application B (données) de la déconnexion.

6) Acquittement [ID d'utilisateur]: le service d'application B (données) acquitte la déconnexion.

7) Notification de déconnexion [ID de dispositif]: le système de gestion IdM informe le service d'application A (VoIP) de la déconnexion.

8) Acquittement [ID d'utilisateur]: le service d'application A (VoIP) acquitte la déconnexion.

9) Acquittement de déconnexion unique [ID d'utilisateur]: le système de gestion IdM envoie un acquittement à l'utilisateur pour confirmer la déconnexion de tous les services d'application actifs dans la session.

II.5 Corrélation d'informations d'identité réparties pour la garantie d'authentification multifacteurs

II.5.1 Aperçu

Ce cas d'utilisation illustre l'utilisation de la gestion IdM pour corréler et lier plusieurs informations d'identité (par exemple identificateurs, justificatifs et attributs) afin de garantir l'identité d'un utilisateur final/abonné. Ainsi, les informations d'identité associées à un abonné (par exemple ID d'utilisateur) et au dispositif d'abonné (par exemple ID de dispositif) et les informations d'emplacement peuvent être corrélées pour fournir un niveau de garantie plus élevé concernant l'abonné.

II.5.2 Exemple de cas d'utilisation

La Figure II.6 illustre un exemple de cas d'utilisation dans lequel l'identité de l'utilisateur et l'identité du dispositif sont reliées et corrélées avec les informations de présence et d'emplacement pour fournir un niveau plus élevé de garantie de l'identité et des déclarations associées à l'identité.

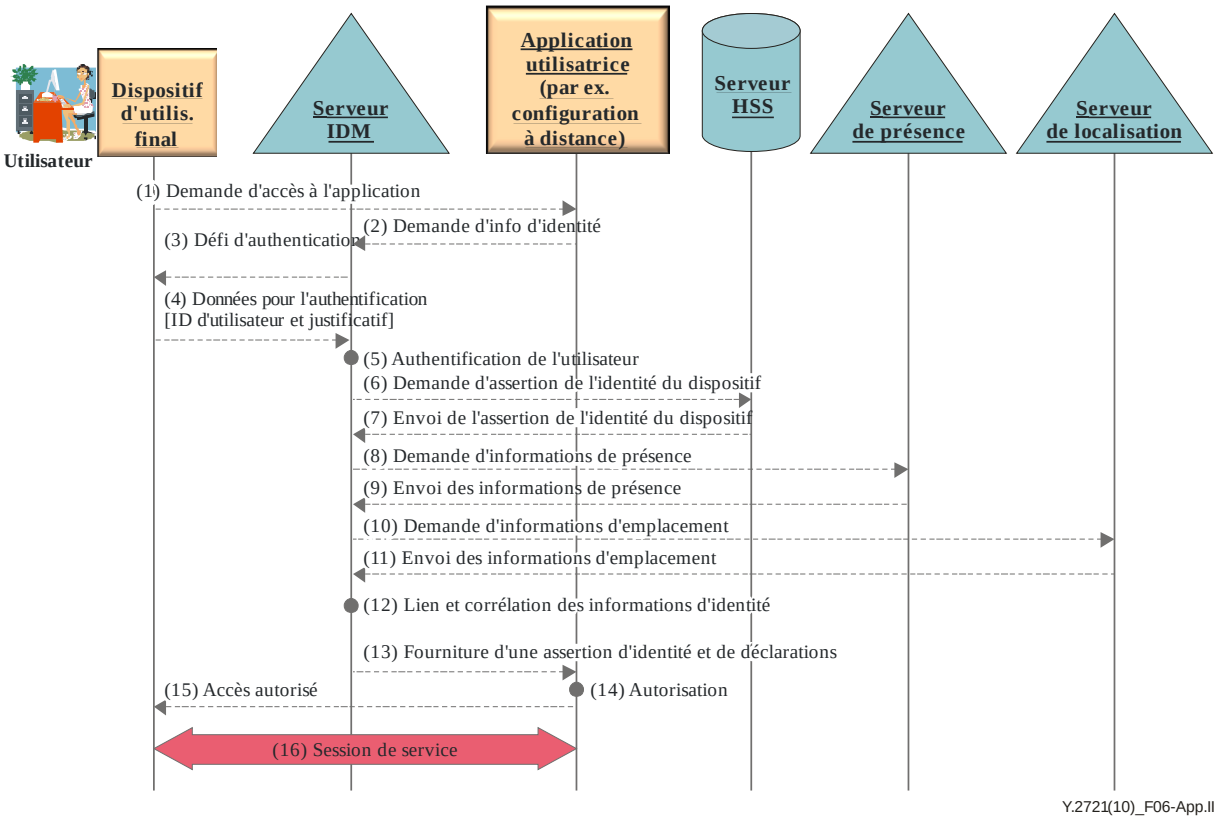


Figure II.6 – Corrélation d'informations d'identité

Dans cet exemple, l'utilisateur final/abonné tente d'accéder à une application qui nécessite un niveau élevé de garantie de l'identité d'utilisateur et des privilèges associés à l'identité car l'accès par un utilisateur non autorisé à l'application ou à la ressource risque de coûter cher sur le plan de la sécurité.

Les flux d'appel sont les suivants:

1) L'utilisateur demande à accéder à l'application.

2) L'application demande au serveur de gestion IdM des assertions de l'identité de l'utilisateur et des déclarations associées à l'identité.

3) Le serveur de gestion IdM envoie un défi d'authentification à l'utilisateur.

4) L'utilisateur fournit au serveur de gestion IdM des données pour l'authentification (par exemple ID d'utilisateur et justificatifs).

5) Le serveur de gestion IdM authentifie l'utilisateur.

6) Le serveur de gestion IdM demande au serveur HSS une assertion de l'identité du dispositif de l'utilisateur. Il est à noter que l'on suppose que l'enregistrement du dispositif de l'utilisateur dans le réseau et son authentification par le réseau se font selon les procédures normales.

7) Le serveur HSS envoie une assertion de l'identité du dispositif de l'utilisateur.

8) Le serveur de gestion IdM demande des informations de présence au serveur de présence.

9) Le serveur de présence fournit les informations de présence au serveur de gestion IdM.

10) Le serveur de gestion IdM demande des informations d'emplacement au serveur de localisation.

11) Le serveur de localisation fournit les informations d'emplacement au serveur de gestion IdM.

12) Le serveur de gestion IdM relie les informations d'identité de l'utilisateur et d'identité du dispositif de l'utilisateur. L'identité combinée est corrélée avec les informations de présence et d'emplacement afin de vérifier les déclarations (par exemple les privilèges) associées à l'identité.

13) Le serveur de gestion IdM fournit à l'application des assertions de l'identité de l'utilisateur et des déclarations associées à l'identité.

14) L'application détermine si l'utilisateur est autorisé à accéder.

15) L'utilisateur obtient l'accès à l'application.

16) La session de service est établie.

II.6 Contrôle par l'utilisateur des informations d'identification personnelle (par exemple préférences) à travers des domaines de fournisseurs de réseau/service homologues

II.6.1 Aperçu

La protection des informations PII est très importante pour les utilisateurs finals/abonnés. Un aspect important de la gestion IdM est de permettre aux utilisateurs finals/abonnés de communiquer aux fournisseurs de service et aux fournisseurs IdSP des informations au sujet des conditions, restrictions, consentements et autorisations concernant la création, la collecte, l'utilisation et la diffusion de leurs informations d'identité.

II.6.2 Description du cas d'utilisation

Ce cas d'utilisation a trait à la mise en application des politiques applicables, par exemple des politiques concernant l'anonymat ou le pseudonymat.

La Figure II.7 illustre un exemple de cas d'utilisation dans lequel un utilisateur demande l'anonymat.

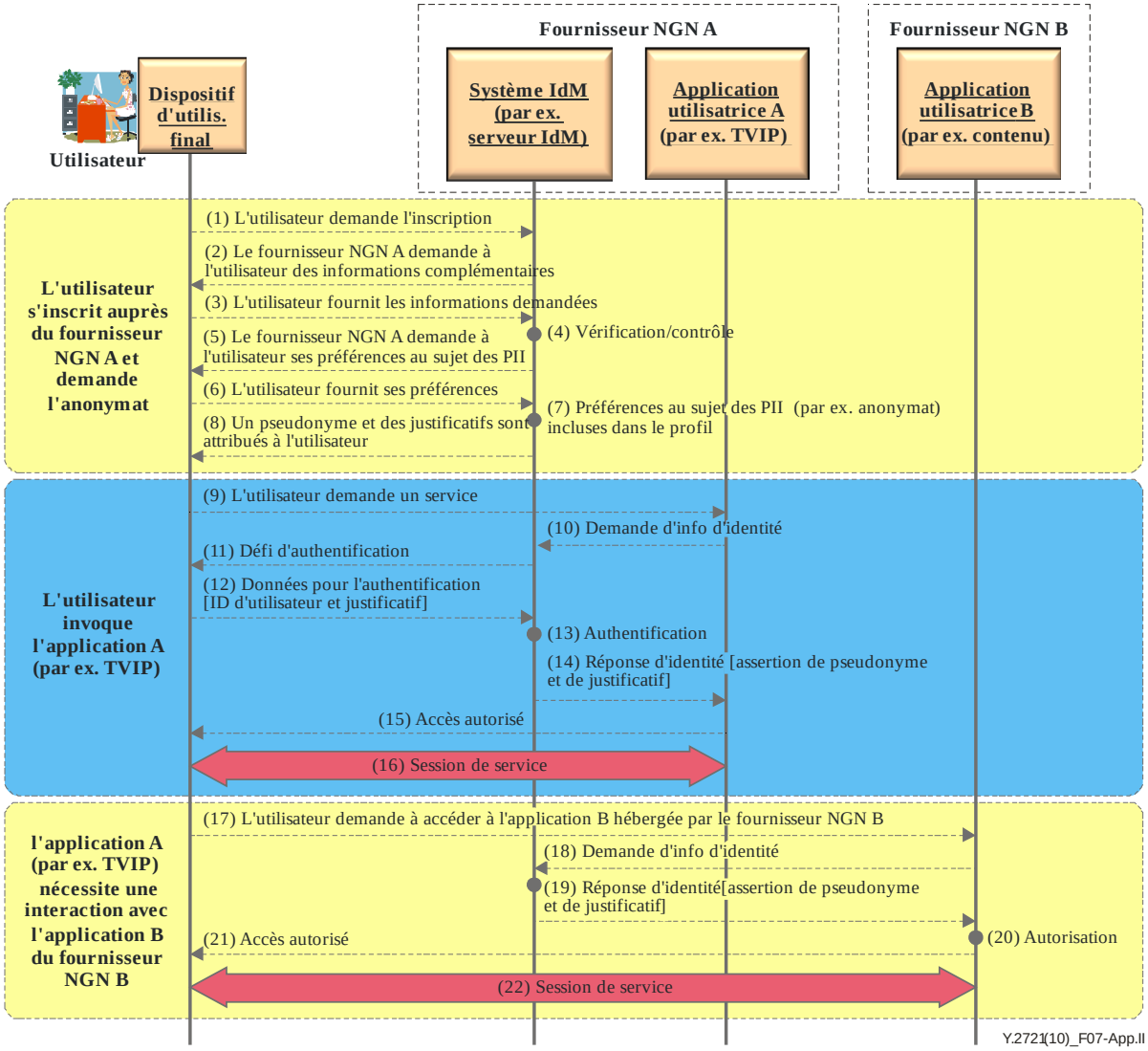


Figure II.7 – Anonymat

NOTE – Le terme "système de gestion IdM" est un terme générique désignant n'importe quel élément de réseau susceptible de fournir des fonctions de gestion IdM, avec diverses possibilités de réalisation/mise en œuvre.

Dans l'exemple de cas d'utilisation, un fournisseur NGN (le fournisseur NGN A) attribue un pseudonyme compte tenu de la demande d'anonymat adressée par l'utilisateur final/abonné. Le pseudonyme est utilisé pour les interactions avec le fournisseur NGN B afin de protéger les informations d'identification personnelle de l'utilisateur final/abonné.

Les flux d'appel sont les suivants:

1) L'utilisateur demande son inscription auprès du fournisseur NGN A.
2) Le fournisseur NGN A demande à l'utilisateur des informations complémentaires.
3) L'utilisateur fournit les informations demandées au fournisseur NGN A.
4) Le fournisseur NGN A vérifie et contrôle les informations.
5) Le fournisseur NGN A demande à l'utilisateur ses préférences au sujet des informations d'identification personnelle (PII).
6) L'utilisateur indique qu'il préfère l'anonymat.
7) Le fournisseur NGN A inclut la préférence d'anonymat dans les informations de profil de l'utilisateur.

8) Un pseudonyme et un justificatif sont attribués à l'utilisateur.

9) L'utilisateur invoque l'application A (par ex. TVIP) hébergée par le fournisseur NGN A.

10) L'application utilisatrice A demande au système de gestion IdM (par exemple au serveur de gestion IdM) des informations d'identité au sujet de l'utilisateur.

11) Le système de gestion IdM envoie un défi d'authentification à l'utilisateur.

12) L'utilisateur fournit les données pour l'authentification au système de gestion IdM (par exemple ID d'utilisateur et justificatif).

13) Le système de gestion IdM authentifie l'utilisateur.

14) Le système de gestion IdM envoie des assertions de l'identité d'utilisateur et des justificatifs à l'application utilisatrice A

NOTE – Seules des informations relatives au pseudonyme sont fournies et ce, en application de la politique concernant l'anonymat.

15) L'utilisateur est autorisé à accéder à l'application A.

16) Session de service.

17) L'utilisateur demande à accéder à l'application B hébergée par le fournisseur NGN B.

18) L'application B demande au système de gestion IdM une assertion de l'identité de l'utilisateur et des déclarations associées.

19) Le système de gestion IdM fournit une assertion de l'identité de l'utilisateur et des déclarations associées. Seules des informations relatives au pseudonyme sont fournies et ce, en application de la politique concernant l'anonymat.

20) L'application B vérifie les informations en vue de l'autorisation.

21) L'autorisation d'accès est accordée à l'utilisateur.

22) La session de service est établie.

II.7 Relais/mappage entre systèmes de gestion IdM hétérogènes

II.7.1 Aperçu

Afin qu'un utilisateur puisse recevoir plusieurs services offerts par divers composants des réseaux NGN, il faut que les réseaux NGN soient dotés de mécanismes permettant d'assurer le relais entre les divers systèmes de gestion IdM. Cette nécessité est illustrée par un cas d'utilisation décrit dans le § II.7.2.

II.7.2 Description du cas d'utilisation

Ce scénario décrit l'accès par un abonné d'un réseau NGN à une ressource (par exemple un serveur d'annuaire) située dans un réseau d'entreprise à l'aide de son combiné. Comme le réseau NGN et le réseau d'entreprise emploient des mécanismes de gestion IdM différents, un relais entre les systèmes de gestion IdM de ces réseaux est nécessaire.

Les entités suivantes interviennent dans un exemple illustrant le scénario:

- Le système de gestion IdM du réseau NGN. Ce système est modifié de manière non seulement à prendre en charge l'authentification mutuelle AKA du combiné de l'utilisateur mais aussi à pouvoir fournir à l'utilisateur les justificatifs pour l'authentification auprès du système de gestion IdM du réseau d'entreprise.
- Le système de gestion IdM du réseau d'entreprise (par exemple centre de distribution de clés).
- Le serveur d'annuaire de l'entreprise (EDS) situé dans le réseau d'entreprise.
- Le combiné de l'utilisateur.

- Les interactions entre ces entités sont les suivantes:
  - Le combiné de l'utilisateur et le réseau mobile s'authentifient en utilisant la méthode AKA.
  - L'utilisateur utilise son combiné pour envoyer une demande au serveur d'annuaire de l'entreprise (EDS) situé dans le réseau d'entreprise.
  - Le serveur EDS répond par une demande d'authentification.
  - L'utilisateur obtient du système de gestion IdM du réseau NGN les justificatifs d'authentification (par exemple un ticket Kerberos), qui sont basés sur les résultats de l'authentification AKA et sont valables pour l'authentification auprès du système de gestion IdM de l'entreprise.

Par exemple, le combiné de l'utilisateur obtient un ticket pour le centre de distribution de clés (KDC) du réseau d'entreprise. Plus précisément, le ticket permet à l'utilisateur d'être authentifié par le serveur distributeur de tickets (TGS), qui fait partie du centre KDC.

- L'utilisateur demande au serveur TGS un ticket pour s'authentifier auprès du serveur EDS.
- Le serveur TGS valide les justificatifs présentés et répond à l'utilisateur en lui fournissant un ticket pour le serveur EDS.
- L'utilisateur final répond à la demande d'authentification du serveur EDS en fournissant le ticket reçu du serveur TGS.
- Le serveur EDS authentifie l'utilisateur et répond en fournissant ses propres justificatifs pour l'authentification auprès de l'utilisateur et une confirmation du service demandé. Après avoir validé les justificatifs du serveur EDS, l'utilisateur peut accéder à ce serveur.

II.7.3 Conséquences

- Le système de gestion IdM du réseau NGN doit prendre en charge le mécanisme d'authentification AKA et le mécanisme d'authentification (par exemple Kerberos) utilisé par le réseau d'entreprise.
- Le système de gestion IdM du réseau NGN doit être capable de délivrer des justificatifs d'authentification (par exemple un ticket Kerberos) au dispositif de l'utilisateur final pour permettre l'authentification de l'utilisateur auprès du système de gestion IdM de l'entreprise.
- Le système de gestion IdM du réseau NGN doit gérer l'identité et les justificatifs de l'utilisateur.
- Le système de gestion IdM de l'entreprise doit gérer l'identité et les justificatifs du serveur.

NOTE – a) Aucune nouvelle capacité n'est nécessaire dans les réseaux 3G (qui peuvent donc servir d'exemple); b) Les exigences énoncées ici s'appliquent spécifiquement pour la prise en charge du cas d'utilisation ci-dessus.

II.8 Prise en charge de services issus de la convergence (par exemple accès fixe et mobile) à l'intérieur du réseau d'un fournisseur de service

II.8.1 Aperçu

Les réseaux de prochaine génération promettent notamment de prendre en charge une multitude de services issus de la convergence sur des réseaux à accès fixe et mobile. Ainsi, un utilisateur aurait la possibilité d'invoquer un service en utilisant le dispositif d'accès et le réseau de son choix à un moment donné. (Quant au fournisseur de service, il élargirait sa clientèle et augmenterait ses recettes.) Etant donné que les mécanismes de sécurité sous-jacents adaptés aux environnements fixe et mobile sont généralement différents, il serait particulièrement utile de disposer d'un système de gestion IdM issu de la convergence qui puisse tenir compte des différences. Ce système gèrerait les identités et les justificatifs des utilisateurs finals et des serveurs de réseau indépendamment de la technologie d'accès.

II.8.2 Description du cas d'utilisation

Ce scénario décrit l'accès par un abonné d'un réseau 3G à une ressource (par exemple un serveur de vidéo à la demande) située dans un réseau fixe à l'aide de son combiné. Dans ce scénario, le réseau 3G et la ressource du réseau fixe prennent en charge des mécanismes différents liés à la gestion IdM. Les entités suivantes interviennent dans un exemple illustrant le scénario:

- Le système de gestion IdM du réseau 3G. Ce système est modifié de manière non seulement à prendre en charge l'authentification mutuelle AKA du combiné de l'utilisateur mais aussi à pouvoir fournir à l'utilisateur les justificatifs pour l'authentification auprès du serveur de vidéo à la demande (VoD).
- Le serveur VoD situé dans le réseau fixe.
- Le combiné 3G de l'utilisateur.
- Les interactions entre ces entités sont les suivantes:
  - Le combiné de l'utilisateur et le réseau mobile s'authentifient en utilisant la méthode AKA.
  - L'utilisateur utilise son combiné pour envoyer une demande au serveur VoD.
  - Le serveur VoD répond à l'utilisateur par une demande d'authentification.
  - L'utilisateur obtient les justificatifs d'authentification (par exemple un ticket Kerberos) auprès du système de gestion IdM du réseau 3G, qui génère ces justificatifs sur la base des résultats de l'authentification AKA.
  - L'utilisateur répond au serveur VoD en fournissant les justificatifs d'authentification (un ticket).
  - Le serveur VoD authentifie l'utilisateur et répond en fournissant une confirmation du service demandé.

II.8.3 Conséquences

- Le système de gestion IdM du réseau 3G doit prendre en charge le mécanisme d'authentification AKA et le mécanisme d'authentification (par exemple Kerberos) utilisé par le serveur VoD.
- Le système de gestion IdM doit être capable de délivrer des justificatifs d'authentification (par exemple un ticket) au dispositif de l'utilisateur pour permettre l'authentification de l'utilisateur auprès du serveur VoD.
- Le système de gestion IdM du réseau 3G doit gérer l'identité et les justificatifs de l'utilisateur.
- Le système de gestion IdM du réseau 3G doit gérer l'identité et les justificatifs du serveur VoD.

NOTE – Les exigences énoncées s'appliquent spécifiquement pour la prise en charge du cas d'utilisation présenté.

II.9 Exemple de cas d'utilisation – Authentification et autorisation d'un fournisseur NGN par un utilisateur (authentification mutuelle et autorisation)

La Figure II.8 illustre un exemple de cas d'utilisation portant sur l'authentification d'un fournisseur NGN par un utilisateur. Dans cet exemple, on se place dans un environnement de service ouvert dans lequel les fournisseurs NGN peuvent faire la publicité de services auprès de l'utilisateur. Cet exemple de cas d'utilisation illustre le fait que l'utilisateur dispose de capacités insuffisantes ou ne dispose pas de capacités pour authentifier et autoriser des fournisseurs NGN (ou pour une authentification mutuelle) dans un environnement de service ouvert et multifournisseur.

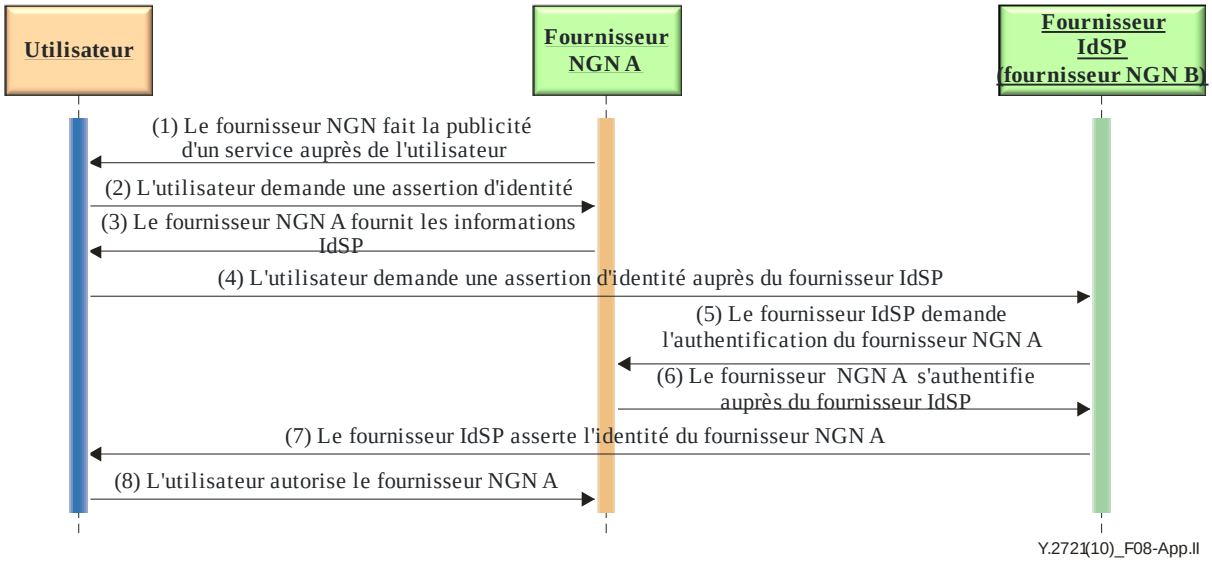


Figure II.8 – Exemple de cas d'utilisation: Authentification et autorisation d'un fournisseur NGN par un utilisateur

Les flux d'appel sont résumés comme suit:

1) Le fournisseur NGN A fait la publicité de services auprès de l'utilisateur.
2) L'utilisateur demande une assertion de l'identité du fournisseur NGN A.
3) Le fournisseur NGN A fournit à l'utilisateur l'adresse d'un fournisseur d'identité IdSP.
4) L'utilisateur demande au fournisseur IdSP une assertion de l'identité du fournisseur NGN A.
5) Le fournisseur IdSP envoie une demande d'authentification au fournisseur NGN A.
6) Le fournisseur NGN A fournit des informations d'authentification.
7) Le fournisseur IdSP envoie à l'utilisateur des informations d'assertion de l'identité du fournisseur NGN A.
8) L'utilisateur autorise le fournisseur NGN A à fournir des services.

NOTE – Dans cet exemple, on ne montre pas les flux liés à l'authentification et à l'autorisation de l'utilisateur par le fournisseur NGN.

II.10 Exemple de cas d'utilisation – Assertion d'utilisateur homologue (transactions non financières)

A l'heure actuelle, il n'existe pas de capacités de gestion IdM des réseaux NGN permettant aux utilisateurs d'authentifier l'origine des communications ou les sources des données. D'une manière générale, les solutions de gestion IdM qui sont en cours de spécification portent principalement sur la gestion IdM pour les transactions financières et le commerce électronique. Les réseaux NGN devront prendre en charge des capacités de gestion IdM pour une plus grande variété de transactions et de communications. C'est particulièrement important pour certains services d'urgence qui devront être pris en charge par les réseaux NGN. La Figure II.9 montre un exemple de cas d'utilisation illustrant la nécessité pour les capacités de gestion IdM des réseaux NGN de permettre aux utilisateurs d'asserter mutuellement leur identité pour des communications entre homologues et des transactions non financières. Par exemple, un utilisateur peut devoir authentifier la source d'un message reçu (par exemple un courrier électronique ou un message instantané), d'une demande de communication (par exemple communication vocale, vidéo ou de données) ou de données reçues. A l'heure actuelle, il n'existe pas de spécifications des réseaux NGN permettant de prendre en charge ces capacités de gestion IdM.

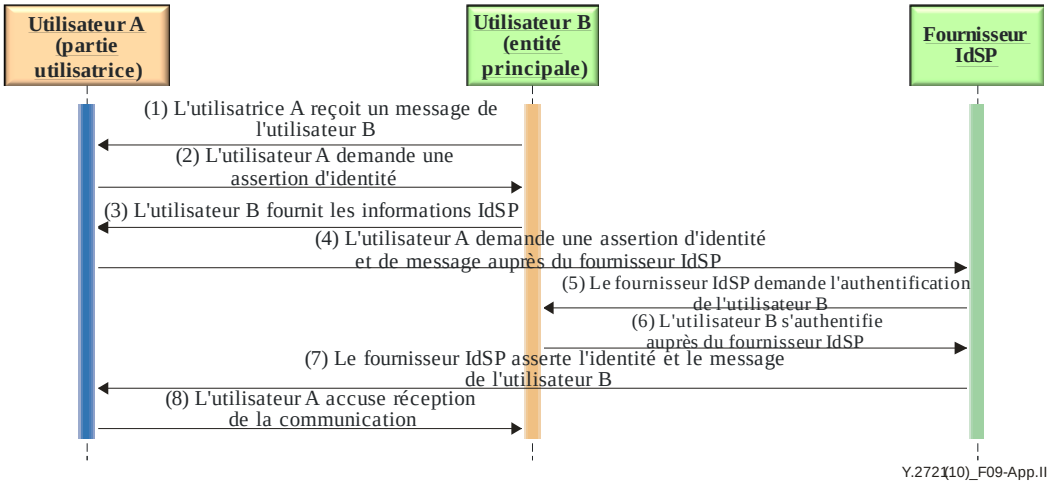


Figure II.9 – Exemple de cas d'utilisation: Assertion d'utilisateur homologue (transaction non financière)

Dans l'exemple de cas d'utilisation illustré sur la Figure II.9, on suppose que l'utilisateur A reçoit un message ou une demande de communication de l'utilisateur B et aimerait asserter l'identité de l'utilisateur B et les données reçues. Les flux d'appel sont résumés comme suit:

1) L'utilisateur A reçoit un message ou une demande de communication de l'utilisateur B.
2) L'utilisateur A demande une assertion de l'identité de l'utilisateur B et l'authentification des informations reçues de l'utilisateur B.
3) L'utilisateur B fournit à l'utilisateur A les informations d'adresse d'un fournisseur IdSP.
4) L'utilisateur A demande au fournisseur IdSP d'asserter l'identité de l'utilisateur B et d'authentifier les informations reçues.
5) Le fournisseur IdSP envoie une demande d'authentification à l'utilisateur B.
6) L'utilisateur B répond est authentifié par le fournisseur IdSP.
7) Le fournisseur IdSP envoie à l'utilisateur A une réponse dans laquelle il asserte l'identité de l'utilisateur B et les informations reçues.
8) L'utilisateur A envoie un accusé de réception de la communication à l'utilisateur B.

II.11 Cas d'utilisation de la gestion IdM – Garantie d'identité et d'intégrité du dispositif de l'utilisateur final

Les réseaux NGN prendront en charge divers dispositifs d'utilisateur (par exemple des téléphones fixes, des combinés sans fil, des ordinateurs personnels, des PDA, des boîtiers-adaptateurs de TVIP). Les composants matériels et logiciels des dispositifs rattachés aux réseaux NGN vont des plus simples aux plus complexes. S'ils sont volés ou compromis, ils peuvent être utilisés pour orchestrer diverses attaques.

Des capacités de sécurité spéciales pourraient être conçues et mises en œuvre dans un composant matériel inaltérable des dispositifs d'utilisateur final afin de conserver les données de gestion d'identité sous forme chiffrée et de prendre en charge des capacités de sécurité spécialisées pour valider l'identité et l'intégrité des dispositifs d'utilisateur final. Le présent paragraphe décrit des exemples de cas d'utilisation dans lesquels un composant matériel de sécurité spécialisé pourrait être conçu et mis en œuvre dans les dispositifs d'utilisateur final et utilisé pour prendre en charge des services de gestion d'identité afin:

1) de garantir l'identité des dispositifs d'utilisateur final;

2) de garantir l'intégrité des dispositifs d'utilisateur final (c'est-à-dire vérifier que le logiciel et le matériel configurés n'ont pas été compromis);

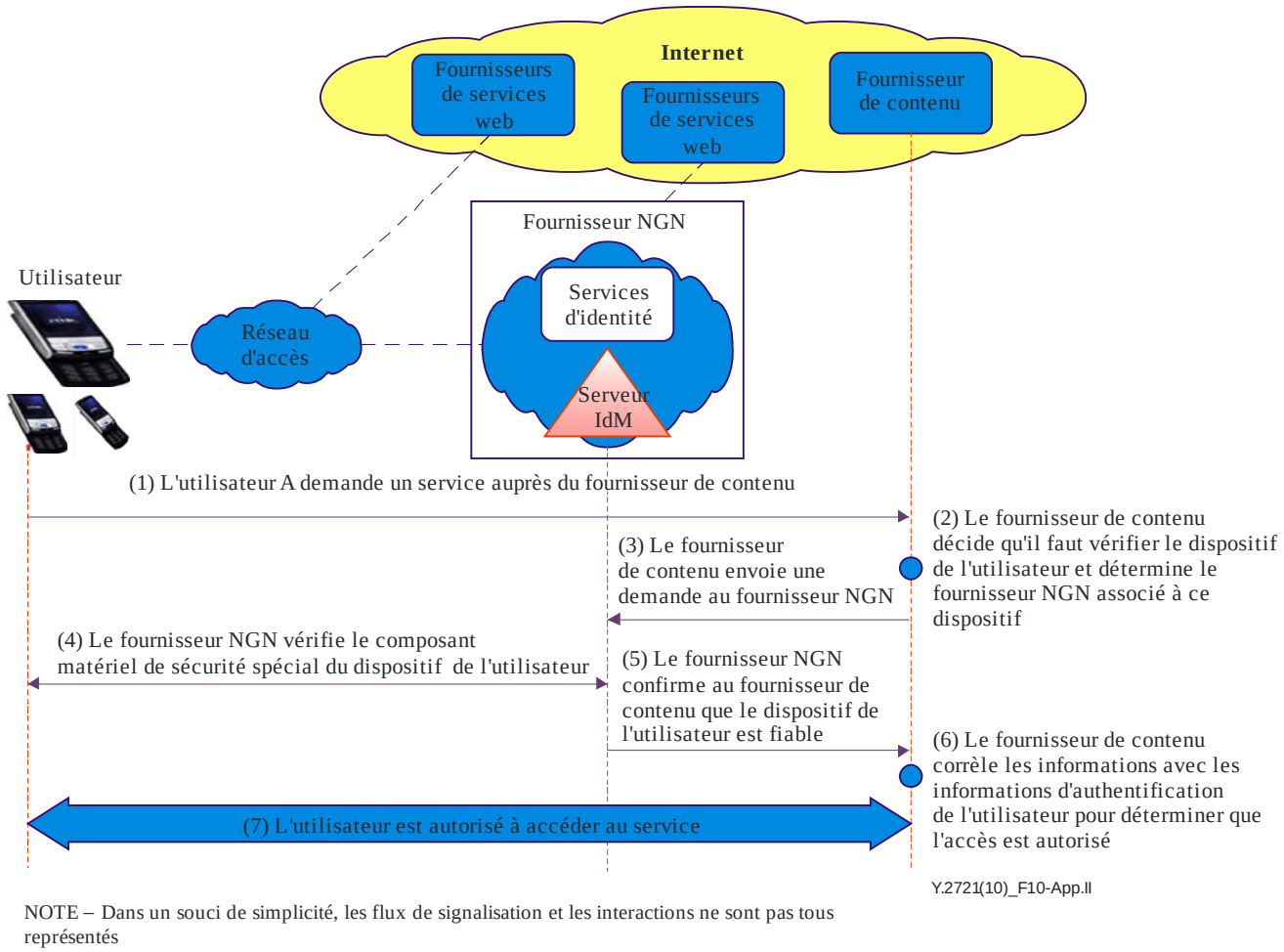
3) de permettre aux utilisateurs de chiffrer et de protéger les informations PII et les autres données sensibles sur les dispositifs des utilisateurs finals.

II.11.1 Exemple de cas d'utilisation – Garantie d'authentification de l'utilisateur et du dispositif

Ce cas d'utilisation repose sur la prise en charge d'un composant matériel inaltérable spécialisé dans le dispositif de l'utilisateur final afin de pouvoir identifier de manière univoque le dispositif. Par exemple, des mots de passe, des clés numériques et des certificats peuvent être stockés dans ce composant afin de pouvoir identifier de manière univoque le dispositif. Le composant matériel spécialisé pourrait prendre en charge des interfaces de programmation d'application (API) normalisées pour permettre la prise en charge de services d'application de sécurité reposant sur l'entité de confiance qu'est ce composant pour le dispositif d'utilisateur final.

L'identification univoque et l'authentification du composant inaltérable pourraient être corrélées avec l'identification et l'authentification de l'utilisateur afin d'avoir un niveau de garantie plus élevé pour le contrôle d'accès dans un environnement avec plusieurs fournisseurs de service.

La Figure II.10 illustre un exemple de cas d'utilisation dans lequel un composant matériel inaltérable spécialisé est conçu et mis en œuvre dans le dispositif de l'utilisateur final afin de pouvoir identifier de manière univoque le dispositif. Dans cet exemple, on suppose que le composant matériel inaltérable spécialisé est contrôlé par le fournisseur NGN dans le cadre d'un accord contractuel avec l'abonné. Sous réserve du consentement exprès de l'utilisateur, le fournisseur IdSP/NGN pourrait offrir des services d'identité à d'autres fournisseurs (par exemple des fournisseurs de contenu, des fournisseurs de services web et des fournisseurs tiers) et à des partenaires pour garantir l'identité et l'authentification du dispositif de l'utilisateur final, ce qui permettrait aux fournisseurs de service d'avoir confiance dans l'identité et l'authentification du dispositif de l'utilisateur final. Les informations sur l'identité et l'authentification du dispositif de l'utilisateur peuvent être corrélées avec l'authentification de l'utilisateur pour avoir un niveau plus élevé de garantie et de confiance.



NOTE – Dans un souci de simplicité, les flux de signalisation et les interactions ne sont pas tous représentés

Figure II.10 – Corrélation de l'authentification d'utilisateur et de dispositif pour la garantie

Les flux d'appel sont résumés ci-après:

1) L'utilisateur demande un service auprès d'un fournisseur de contenu.

2) Le fournisseur de contenu décide qu'il faut vérifier le dispositif de l'utilisateur avant d'autoriser l'accès au service et détermine le fournisseur NGN associé à ce dispositif.

3) Le fournisseur de contenu demande au fournisseur NGN d'asserter l'identité et l'authentification du dispositif de l'utilisateur.

4) Le fournisseur NGN identifie et authentifie le composant matériel de sécurité spécial du dispositif de l'utilisateur (par exemple en vérifiant les certificats stockés dans le composant matériel de sécurité inaltérable du dispositif).

5) Le fournisseur NGN envoie au fournisseur de contenu une réponse validant l'identité et l'authentification du dispositif de l'utilisateur.

6) Le fournisseur de contenu corrèle les informations provenant du fournisseur NGN avec les informations d'authentification de l'utilisateur et détermine que l'accès au service est autorisé.

7) L'utilisateur est autorisé à accéder au service (par exemple contenu).

II.11.2 Exemple de cas d'utilisation – Garantie d'intégrité du dispositif de l'utilisateur

Dans l'environnement de sécurité actuel, les abonnés accèdent au réseau en utilisant différents dispositifs (par exemple des téléphones fixes, des combinés sans fil, des ordinateurs personnels, des PDA, des boîtiers-adaptateurs de TVIP). L'intégrité des dispositifs des utilisateurs finals (par exemple le logiciel et le matériel configurés) pourrait facilement être compromise à l'insu de l'utilisateur/abonné. Les applications Internet courantes (par exemple les navigateurs web et le courrier électronique) et les autres applications qui sont exécutées sur les dispositifs d'abonné et qui permettent aux abonnés d'interagir avec des fonctionnalités de dispositif locales et des services, sont susceptibles de compromettre l'intégrité des dispositifs en introduisant des vulnérabilités. Par exemple, ces applications peuvent présenter des failles de sécurité intrinsèques ou prendre en charge des fonctionnalités téléchargements de fichiers, appliquettes logicielles, modules externes de navigation, liens imbriqués, etc. qui peuvent être exploitées. Les téléchargements de logiciels et de fichiers, en particulier en provenance d'une source non fiable, rendent les dispositifs d'abonné vulnérables aux codes malveillants, vers, virus et chevaux de Troie. Les enregistreurs de frappe (qui enregistrent toutes les saisies au clavier, y compris les noms d'utilisateur et les mots de passe, et qui retransmettent ensuite les informations à un attaquant qui peut les utiliser pour obtenir un accès non autorisé) font partie des types courants de code malveillant, parmi lesquels on trouve aussi les logiciels espions (programmes qui suivent les activités de l'abonné) et les logiciels de publicité (programmes qui affichent des publicités non souhaitées, souvent basées sur des informations collectées dans le cadre de la surveillance d'un abonné). Certains de ces programmes piratent littéralement les dispositifs d'abonné et cachent leur présence en s'intégrant en profondeur dans le système d'exploitation.

Ce cas d'utilisation repose sur la prise en charge d'un composant matériel inaltérable spécialisé dans le dispositif de l'utilisateur final afin de pouvoir contrôler l'intégrité et confirmer l'intégrité du dispositif aux applications et services. Par exemple, ce composant pourrait contenir des algorithmes et des fonctions propres à un fournisseur afin de vérifier si l'intégrité été compromise. Il pourrait inclure un modèle de référence avec un ensemble de paramètres d'intégrité bien connus afin de déterminer le code correct et de fournir des valeurs de référence pour le dispositif. Ces paramètres seraient utilisés pour comparer les valeurs réelles indiquées à la configuration et déterminer si l'unité est conforme.

La Figure II.11 illustre un exemple de cas d'utilisation dans lequel un composant matériel inaltérable spécialisé est conçu et mis en œuvre dans le dispositif de l'utilisateur final afin de pouvoir vérifier l'intégrité du dispositif. Dans cet exemple, on suppose que le composant matériel inaltérable spécialisé est contrôlé par le fournisseur NGN dans le cadre d'un accord contractuel avec l'abonné. Sous réserve du consentement exprès de l'utilisateur, le fournisseur IdSP/NGN pourrait offrir des services d'identité à d'autres fournisseurs (par exemple des fournisseurs de contenu, des fournisseurs de services web et des fournisseurs tiers) et à des partenaires pour valider l'intégrité du dispositif de l'utilisateur final.

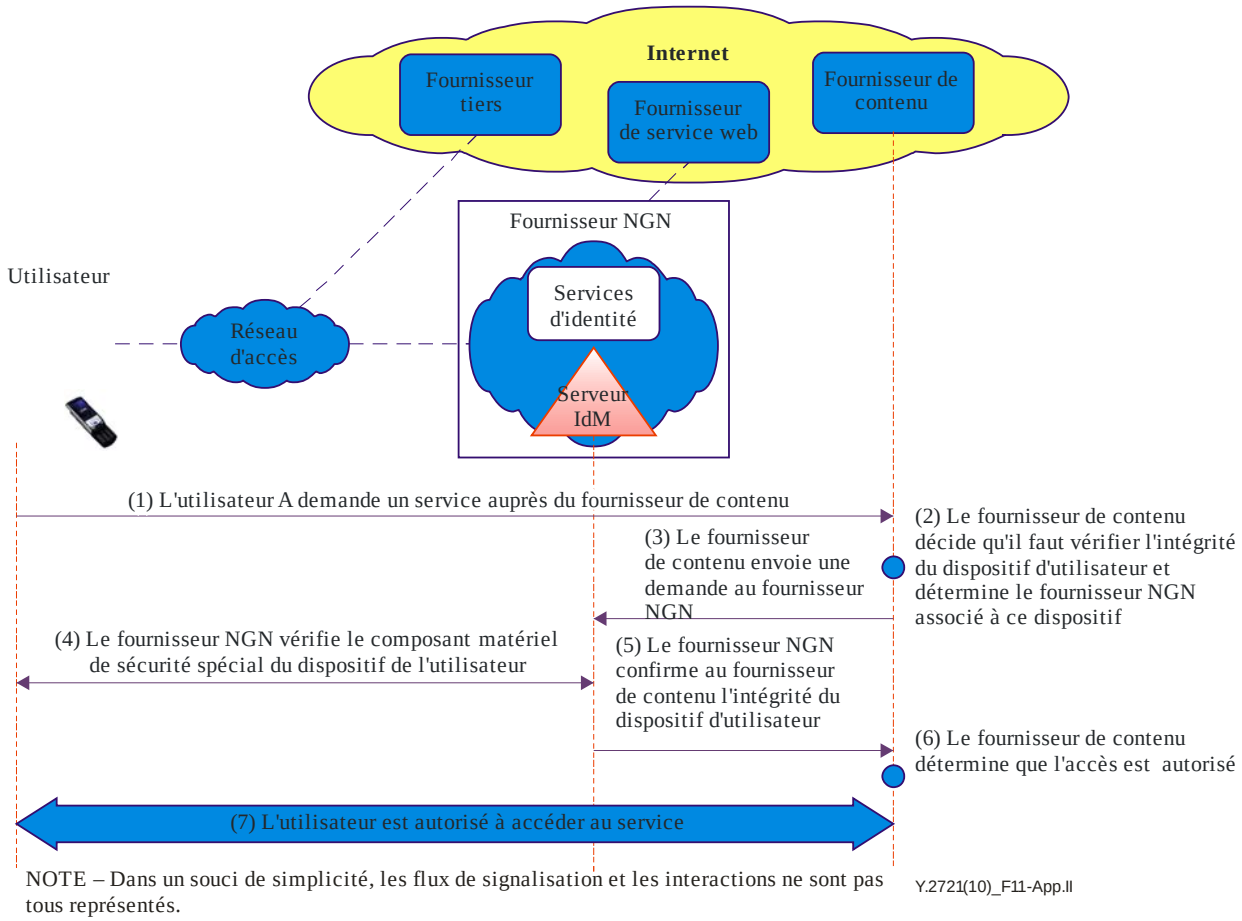


Figure II.11 – Garantie d'intégrité de dispositif

Les flux d'appel sont résumés ci-après:

1) L'utilisateur demande un service auprès du fournisseur de contenu.
2) Le fournisseur de contenu détermine qu'il faut vérifier l'intégrité du dispositif d'utilisateur et détermine le fournisseur NGN associé à ce dispositif.
3) Le fournisseur de contenu demande au fournisseur NGN de lui confirmer l'intégrité du dispositif de l'utilisateur.
4) Le fournisseur NGN interagit avec le composant matériel de sécurité spécial du dispositif de l'utilisateur pour vérifier l'intégrité.
5) Le fournisseur NGN confirme au fournisseur de contenu l'intégrité du dispositif de l'utilisateur.
6) Le fournisseur de contenu détermine que l'accès est autorisé.
7) L'utilisateur est autorisé à accéder au service (par exemple contenu).

II.11.3 Exemple de cas d'utilisation – Chiffrement des informations PII et des fichiers/données sensibles

La perte ou le vol d'un dispositif comportant des informations PII et d'autres données sensibles pourrait entraîner de graves conséquences pour des particuliers, des entreprises privées ou des structures de l'Etat. Le composant matériel spécialisé conçu pour identifier de manière univoque et confirmer l'intégrité de dispositifs fiables pourrait aussi prendre en charge des capacités permettant de chiffrer et de protéger les informations PII et les autres données sensibles sur les dispositifs des utilisateurs finals. Avec des données confidentielles chiffrées, les parties non autorisées ne peuvent pas accéder aux données sur les ordinateurs, téléphones cellulaires ou dispositifs de stockage, ce qui évite d'avoir à apporter des mesures correctives importantes et onéreuses.

Appendice III

Cas d'utilisation de la gestion IdM liés au service de télécommunications d'urgence (ETS)

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

III.1 Introduction

Le présent appendice donne des exemples de cas d'utilisation de la gestion IdM liés au service ETS. Le service ETS est un service qui nécessite un traitement prioritaire. Voir le § 8.4.7.

III.2 Garantie d'authentification reposant sur la combinaison dispositif et utilisateur

L'authentification des utilisateurs autorisés du service ETS est nécessaire pour protéger la disponibilité et l'intégrité du service ETS et des réseaux associés. Deux méthodes d'authentification de base sont actuellement utilisées pour les applications ETS existantes, à savoir:

1) une méthode basée sur le numéro PIN; et

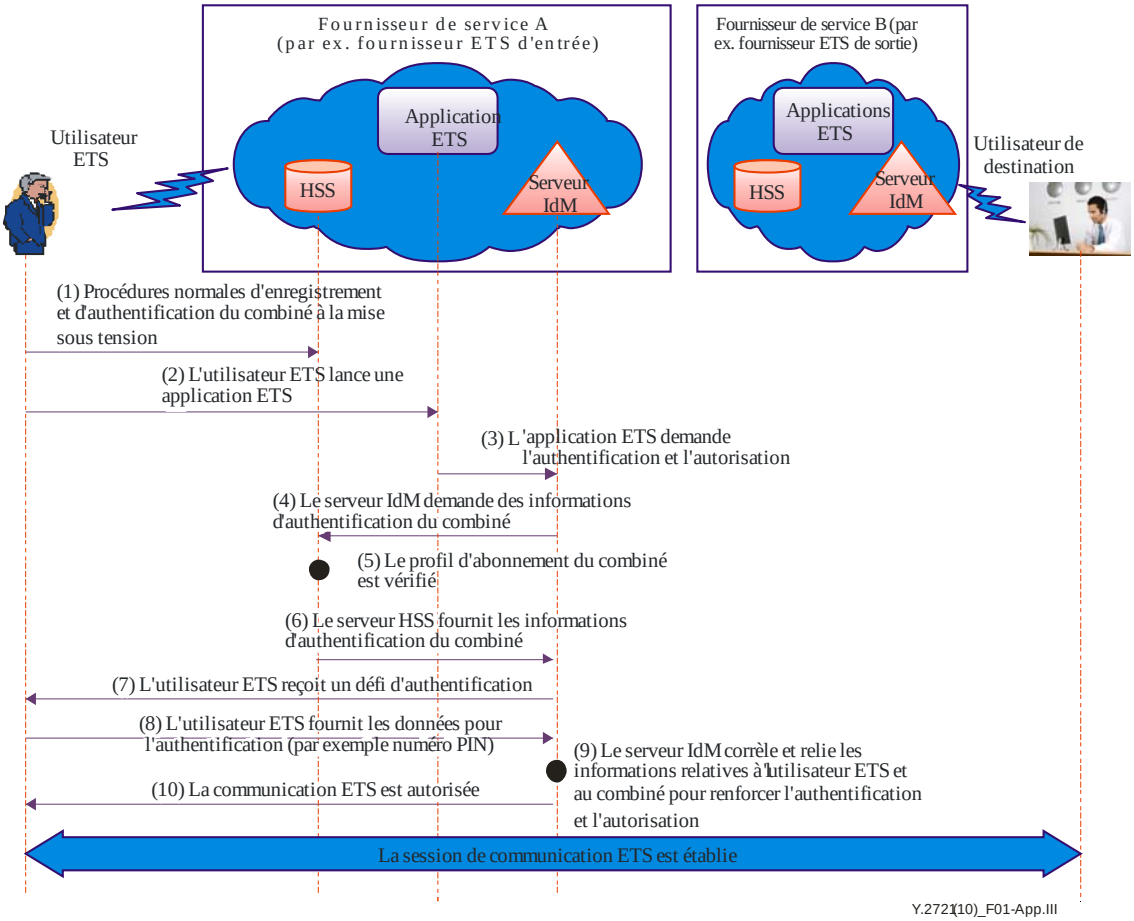
2) une méthode basée sur l'abonnement.

La première méthode repose sur l'utilisation d'un numéro d'identification personnel (PIN) pour l'authentification et l'autorisation. La validation du numéro PIN permet d'authentifier l'utilisateur et par là-même de l'autoriser à utiliser le service ETS. Dans cette méthode, on identifie l'utilisateur mais pas son dispositif. Par conséquent, cette méthode est en principe utilisée dans les cas où l'utilisateur est autorisé à invoquer le service ETS depuis n'importe quel dispositif.

Dans la deuxième méthode, l'authentification et l'autorisation sont fondées sur les informations de profil d'abonnement associées à un terminal ou à un dispositif d'utilisateur final particulier. L'identité du dispositif de l'utilisateur ou du terminal est authentifiée dans le cadre des procédures normales d'enregistrement et d'authentification du fournisseur NGN (c'est-à-dire le fournisseur de service ETS) et, pour l'autorisation de chaque appel/session ETS, on vérifie le profil de l'abonnement au service (c'est-à-dire qu'on vérifie si l'abonnement au service autorise les appels/sessions ETS depuis le dispositif). Dans cette méthode, on authentifie le dispositif de l'utilisateur (c'est-à-dire le combiné sans fil) mais pas l'utilisateur.

Les méthodes simples basées sur le numéro PIN et sur l'abonnement conviennent pour les applications ETS existantes mais pas pour tous les types d'applications ETS dans l'environnement NGN. Plus précisément, des applications telles que les services prioritaires multimédias (par exemple services de données et vidéo) nécessiteront un niveau plus élevé de garantie ou de confiance concernant l'identité de l'utilisateur ETS et le niveau d'autorisation pour accéder à l'application ETS et à sa ressource associée. Par conséquent, outre la prise en charge des méthodes d'authentification existantes basées sur le numéro PIN et sur l'abonnement, le réseau NGN devra aussi prendre en charge des mécanismes renforcés d'authentification et d'autorisation des utilisateurs ETS et de leurs dispositifs.

Une méthode à prendre en considération pour le passage du service ETS (c'est-à-dire des services vocaux prioritaires) dans l'environnement NGN consiste à utiliser la gestion IdM pour corréler et relier l'authentification de l'utilisateur et l'identification et l'authentification du dispositif de l'utilisateur, ce qui permettra de renforcer la garantie (autrement dit la confiance) concernant l'identité et l'autorisation de l'utilisateur pour l'accès au service ETS. Le concept est décrit dans l'exemple général suivant de cas d'utilisation.



NOTE– Dans un souci de simplicité, les flux de signalisation et les interactions ne sont pas tous représentés.

Figure III.1 – Authentification combinée de l'utilisateur et du dispositif

La Figure III.1 montre un exemple de cas d'utilisation dans lequel des fonctions de gestion IdM sont utilisées pour combiner l'authentification de l'utilisateur et du dispositif afin de renforcer la garantie d'autorisation des utilisateurs ETS.

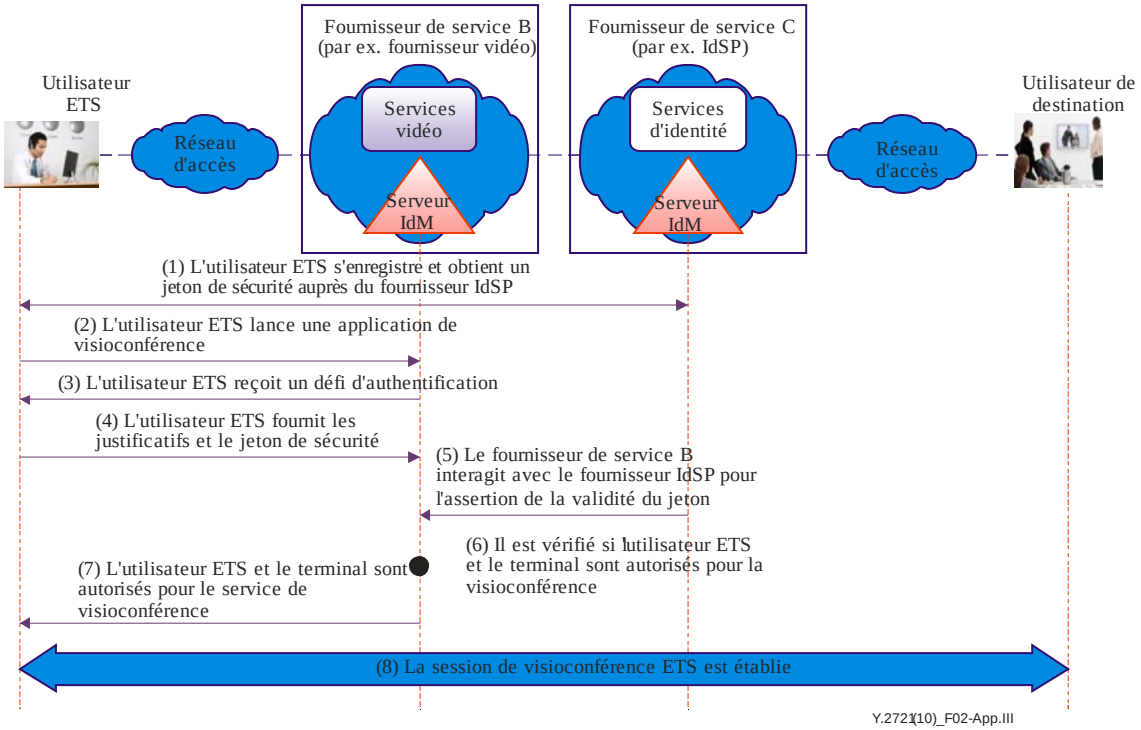
Les flux d'appel sont résumés ci-après:

1) A sa mise sous tension, le combiné de l'utilisateur est enregistré et authentifié selon les procédures normales.
2) L'utilisateur ETS lance une application ETS.
3) L'application ETS demande au serveur de gestion IdM l'authentification et l'autorisation.
4) Le serveur de gestion IdM demande au serveur HSS des informations d'authentification du combiné.
5) Le serveur HSS vérifie le profil d'abonnement du combiné.
6) Le serveur HSS fournit au serveur de gestion IdM les informations d'authentification du combiné.
7) L'utilisateur ETS reçoit un défi d'authentification.
8) L'utilisateur ETS fournit les données pour l'authentification (par exemple numéro PIN)
9) Le serveur de gestion IdM corrèle et relie les informations relatives à l'utilisateur ETS et au combiné pour renforcer l'authentification et l'autorisation.
10) La session de communication ETS est autorisée.

Dans cet exemple, le résultat est un renforcement de la garantie de l'identité de l'utilisateur ETS et de l'autorisation d'utilisation du service. La combinaison de l'authentification du dispositif et de celle de l'utilisateur, qui nécessitera des interactions supplémentaires avec l'utilisateur ETS pour l'authentification, pourrait être considérée comme contraignante. Toutefois, elle ne sera peut-être pas nécessaire pour toutes les sessions ETS. Elle pourrait être envisagée pour les sessions ETS nécessitant un niveau très élevé de garantie.

III.3 Authentification renforcée des utilisateurs ETS pour les services prioritaires de prochaine génération (services prioritaires multimédias)

Avec le passage de l'environnement de communications à un environnement NGN/IMS, les utilisateurs ETS devront suivre le rythme de l'évolution de la technologie et des nouvelles tendances en matière de communications. Par exemple, les utilisateurs ETS sont de plus en plus amenés à utiliser, en plus des communications vocales, des communications telles que des messages instantanés, des messages textuels et des courriers électroniques, pour mener à bien leur mission. D'une manière générale, il existe des initiatives en cours de planification et de développement visant à permettre aux utilisateurs ETS d'obtenir un accès prioritaire aux services multimédias tels que les services vocaux, vidéo et de données. Toutefois, les mécanismes basés sur le numéro PIN et sur l'abonnement utilisés pour le service ETS dans l'environnement RTPC ne conviendront pas pour les services multimédias dans l'environnement NGN/IMS. Plus précisément, des applications telles que les services prioritaires multimédias (par exemple services vidéo et de données) nécessiteront un niveau plus élevé de garantie ou de confiance concernant l'identité de l'utilisateur ETS et le niveau d'autorisation pour accéder à l'application ETS et à sa ressource associée en raison des menaces et des risques accrus concernant la sécurité de l'environnement NGN en général. De plus, contrairement au service ETS existant pris en charge dans le RTPC, l'accès aux services prioritaires multimédias de prochaine génération ne devrait être autorisé qu'à certains utilisateurs ETS. Par ailleurs, étant donné que l'objectif général des utilisateurs ETS est de disposer d'un accès facile et simple partout, à tout moment et depuis n'importe quel dispositif, il est important d'envisager des mécanismes de gestion IdM plus évolués et d'en tirer parti selon qu'il conviendra. Un niveau élevé de garantie de l'identité de l'utilisateur ETS sera essentiel pour protéger l'intégrité et la disponibilité des services multimédias ETS et des ressources ainsi que toute l'infrastructure NGN/IMS dans son ensemble lors des situations d'urgence et de catastrophe. Les applications multimédias vidéo et de données (par exemple les téléchargements d'informations sur le web ou de clips vidéo) sont gourmandes en largeur de bande et en ressources si on les compare aux applications vocales. En l'absence de contrôles appropriés, l'accès non autorisé à des applications vidéo et de données ETS pourrait avoir des conséquences néfastes pour les applications ETS proprement dites et pour toute l'infrastructure de communication en général. Par exemple, l'accès non autorisé à une application ETS gourmande en ressources risque d'être utilisé pour provoquer des encombrements dans le réseau ou pour réaliser des attaques par déni de service. Par conséquent, il convient d'envisager des méthodes plus sophistiquées utilisant des jetons de sécurité spéciaux, des certificats numériques, des capacités de reconnaissance vocale ou des capacités biométriques pour authentifier et autoriser les utilisateurs ETS et/ou les terminaux.



NOTE – Dans un souci de simplicité, les flux de signalisation et les interactions ne sont pas tous représentés.

Figure III.2 – Authentification renforcée pour les services prioritaires de prochaine génération

La Figure III.2 illustre un exemple de cas d'utilisation relatif à l'authentification renforcée des utilisateurs autorisés pour les services prioritaires multimédias de prochaine génération (par exemple visioconférences). Dans ce cas d'utilisation, on suppose que le justificatif d'identité (à savoir le jeton de sécurité ou le certificat numérique) est fourni par un fournisseur IdSP qui est différent du fournisseur du service multimédia (même s'il est possible que le fournisseur de service et le fournisseur IdSP/NGN soient une seule et même entité). Si le fournisseur IdSP et le fournisseur de service sont différents, il faut établir au préalable les accords nécessaires concernant les activités et la confiance. Il faut aussi prévoir une authentification mutuelle entre le fournisseur IdSP et le fournisseur de service.

Les flux d'appel sont résumés ci-après:

1) L'utilisateur ETS s'enregistre et obtient un justificatif (à savoir un jeton de sécurité ou un certificat numérique) identifiant l'utilisateur ETS et les privilèges relatifs aux services multimédias.

2) L'utilisateur ETS lance une application de visioconférence.

3) L'utilisateur ETS reçoit un défi d'authentification.

4) L'utilisateur ETS fournit les justificatifs (par exemple jeton de sécurité ou certificat numérique) pour l'authentification.

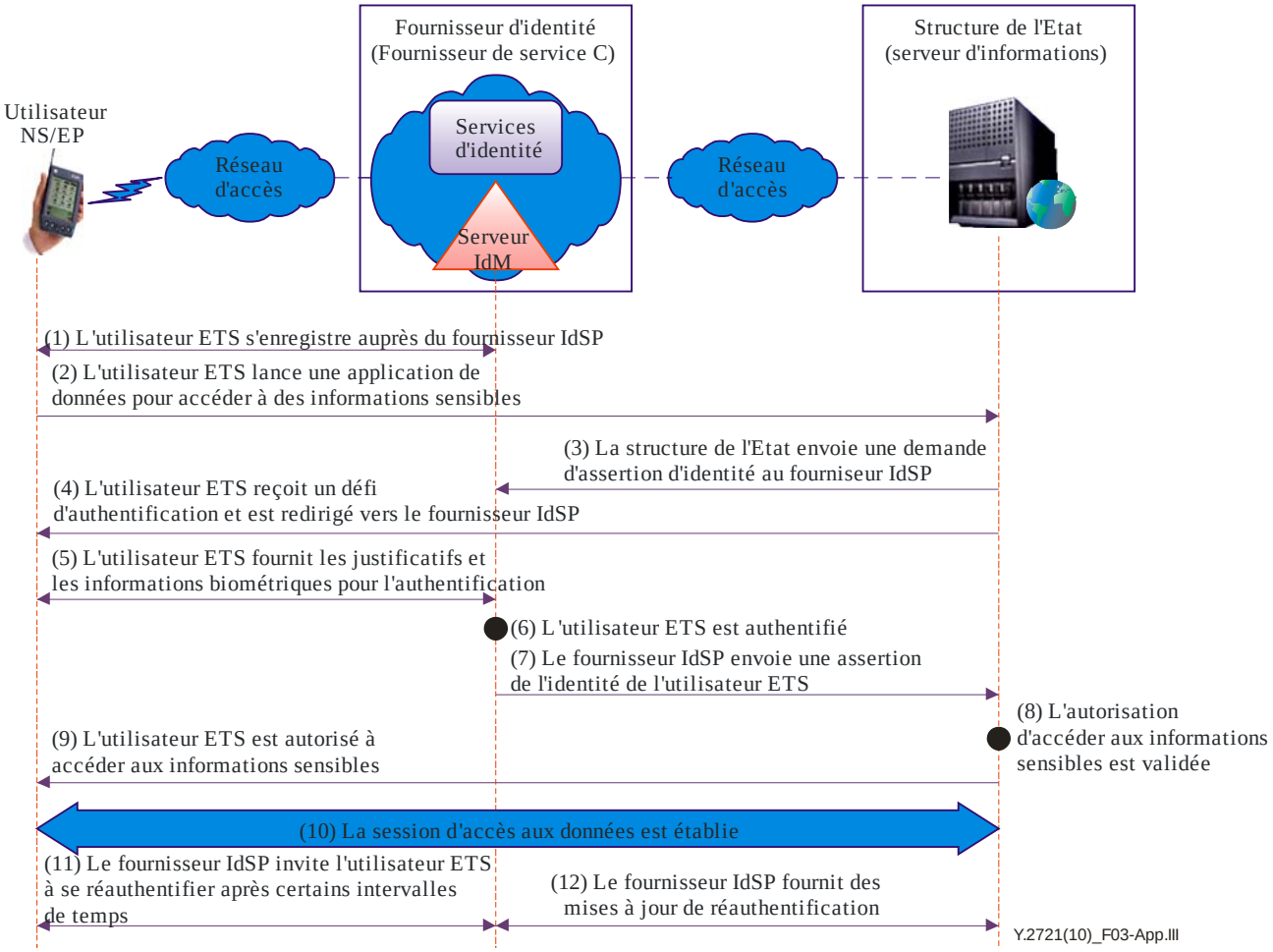
5) Le fournisseur de service B interagit avec le fournisseur de service d'identité (IdSP) pour demander la validation des justificatifs (par exemple jeton de sécurité ou certificat numérique).

6) Le fournisseur de service B traite et vérifie les informations pour déterminer si l'utilisateur ETS et le terminal sont autorisés pour les services prioritaires multimédias.

7) L'utilisateur ETS est autorisé à lancer le service prioritaire multimédia (par exemple visioconférence) après l'authentification réussie.

8) La session multimédia est établie.

Pour certaines communications multimédias de prochaine génération, il pourra être nécessaire d'utiliser des informations biométriques pour authentifier les utilisateurs ETS autorisés. Par exemple, pour certaines informations sensibles, il pourra être nécessaire de faire en sorte que celles-ci ne puisse être échangées qu'entre certains utilisateurs ETS autorisés. En pareil cas, un niveau élevé de confiance dans la validation de l'identité de l'utilisateur ETS est essentielle et, pour cela, on pourra envisager des mécanismes biométriques pour la validation.



NOTE – Dans un souci de simplicité, les flux de signalisation et les interactions ne sont pas tous représentés.

Figure III.3 – Exemple de cas d'utilisation avec des données biométriques

La Figure III.3 montre un exemple de cas d'utilisation avec des données biométriques. Dans cet exemple, on suppose que le combiné de l'utilisateur est équipé d'une capacité permettant de lire les informations biométriques. On suppose aussi que l'utilisateur ETS effectue un pré-enregistrement auprès du fournisseur IdSP et que les informations biométriques nécessaires sont obtenues et stockées. Il est à noter qu'il est également possible que les services d'identité (par exemple enregistrement et conservation de l'identité de l'utilisateur ETS et des informations biométriques) soient hébergés et fournis par la structure de l'Etat plutôt que d'utiliser les services d'un fournisseur de service tiers. Les flux d'appel sont résumés ci-après:

1) L'utilisateur ETS s'enregistre auprès du fournisseur IdSP pour activer le service d'authentification biométrique. On suppose que le processus nécessaire pour collecter et

vérifier les informations biométriques et autres informations d'identité a déjà eu lieu (par exemple enregistrement en personne).

2) L'utilisateur ETS lance une communication pour accéder à distance à une base de données de la structure de l'Etat hébergeant des informations sensibles.

3) La politique de sécurité de la structure de l'Etat indique qu'un niveau élevé de garantie est nécessaire pour permettre l'accès et lance une procédure de redirection vers le fournisseur IdSP.

4) L'utilisateur ETS reçoit un défi d'authentification et est redirigé vers le fournisseur IdSP.

5) L'utilisateur ETS fournit les données pour l'authentification, par exemple, en posant son pouce sur un scanner biométrique spécial intégré au combiné sans fil.

6) Le fournisseur IdSP utilise ces données pour authentifier l'utilisateur ETS.

7) Le fournisseur IdSP envoie à la structure de l'Etat les informations d'assertion de l'identité de l'utilisateur ETS.

8) La structure de l'Etat vérifie si l'utilisateur ETS est autorisé à accéder au serveur d'information hébergeant des données sensibles.

9) L'utilisateur ETS est autorisé à accéder.

10) La session d'accès aux données est établie.

11) Le fournisseur IdSP invite l'utilisateur ETS à se réauthentifier après un intervalle de temps spécifique en application de la politique de sécurité relative à l'accès au serveur d'information de la structure de l'Etat.

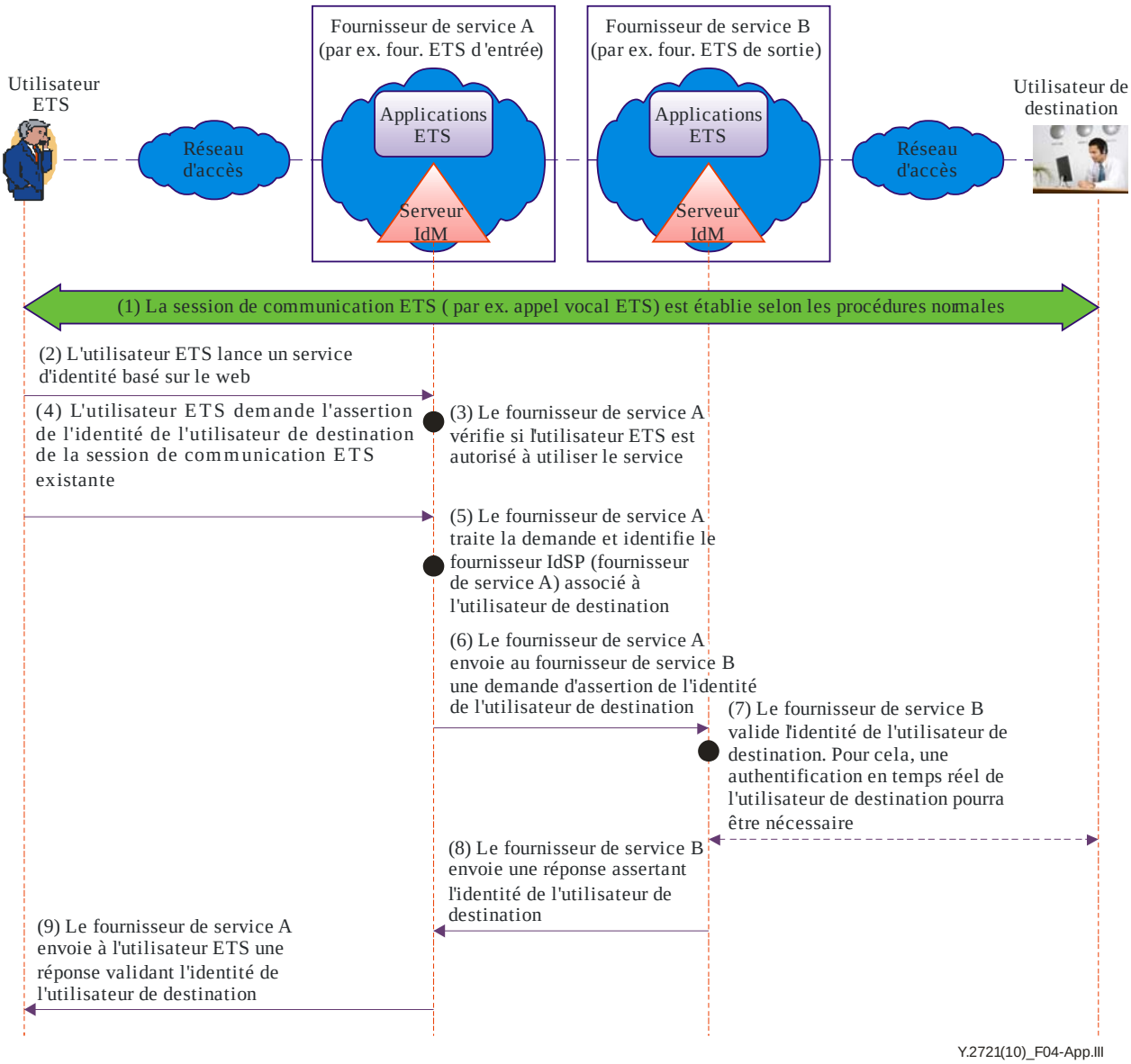
12) Le fournisseur IdSP fournit des informations sur la réauthentification de l'utilisateur ETS à la structure de l'Etat.

III.4 Authentification de l'appelé et de la source des communications de données

A l'heure actuelle, il n'existe pas, dans le cadre des applications ETS proprement dites, de mécanismes spécifiques permettant d'authentifier l'appelé de la session de communication (à savoir le côté destination de l'appel ETS). Dans l'environnement RTPC fermé, ce n'était pas vraiment un problème. Mais avec le passage à l'environnement NGN/IMS avec transport IP, une falsification du numéro de l'appelé et des informations de routage est possible, ce qui entraîne des menaces d'usurpation d'identité.

Dans le futur, il pourrait être possible de tirer parti des services de gestion d'identité offerts par les fournisseurs de service de communication (CSP) et les fournisseurs de service tiers pour authentifier l'appelé ou le côté destination des sessions de communication ETS. Plus précisément, le fournisseur de service ETS pourrait prendre en charge des capacités de gestion IdM permettant de fournir des services d'identité visant à authentifier les utilisateurs et à asserter leurs identités, par exemple de simples vérifications de la ligne ou du nom de l'appelant ou l'utilisation de mécanismes d'authentification forte reposant sur des jetons de sécurité, des cartes à puce ou des certificats numériques pour garantir l'identité de l'utilisateur.

La Figure III.4 illustre un exemple de cas d'utilisation relatif à l'assertion de l'utilisateur de destination d'une session de communication ETS (par exemple un appel vocal ETS). Plus précisément, on suppose dans ce cas d'utilisation que l'utilisateur ETS a effectué un pré-enregistrement auprès du fournisseur de service ETS pour les services d'identité basés sur le web. Après avoir établi une communication ETS (par exemple un appel vocal ETS) à destination d'un utilisateur dans le réseau public, l'utilisateur ETS lance un service d'identité par le biais d'un portail web pour vérifier l'identité de l'utilisateur de destination à l'autre extrémité de la communication ETS. Dans cet exemple de cas d'utilisation, l'établissement de la session de communication ETS est indépendant du service d'identité qui est utilisé pour garantir l'identité de l'utilisateur de destination.



NOTE – Dans un souci de simplicité, les flux de signalisation et les interactions ne sont pas tous représentés.

Figure III.4 – Assertion de l'identité de l'utilisateur de destination

Le flux d'appel et les interactions sont résumés ci-après:

1) L'utilisateur ETS lance une session de communication ETS (par exemple un appel vocal ETS). Cette session est établie selon les procédures normales.

2) L'utilisateur ETS lance un service d'identité basé sur le web (par exemple via un portail web du fournisseur de service A, le fournisseur ETS d'entrée) pour valider l'utilisateur côté destination de la session de communication ETS établie.

3) Le fournisseur de service A vérifie si l'utilisateur ETS est autorisé à utiliser le service.

4) L'utilisateur ETS demande la validation de l'identité de l'utilisateur côté destination de la session de communication établie.

5) Le fournisseur de service A traite la demande et détermine le fournisseur IdSP associé à l'utilisateur de destination (c'est-à-dire le fournisseur ETS de sortie).

6) Le fournisseur de service A envoie au fournisseur de service B une demande d'assertion de l'identité de l'utilisateur de destination.

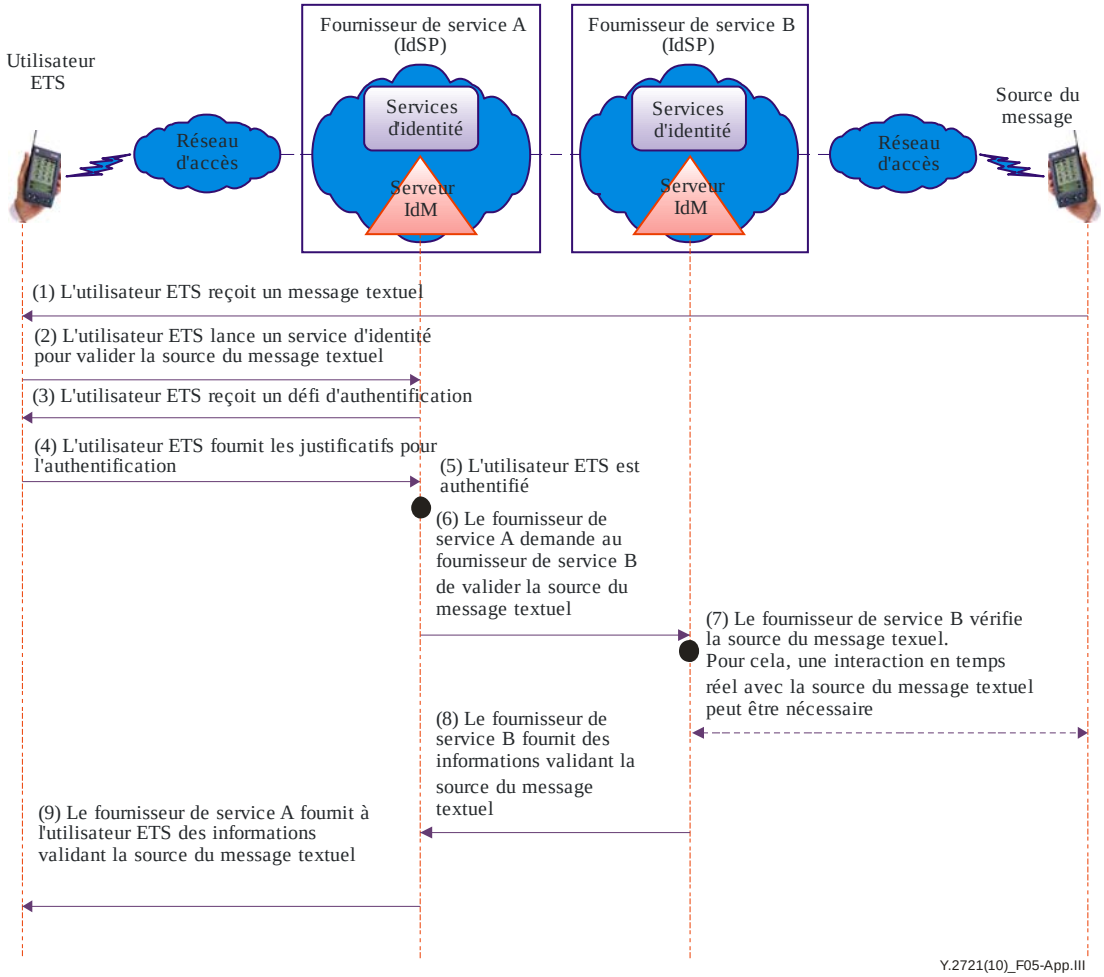
7) Le fournisseur de service B valide l'identité de l'utilisateur de destination. Pour cela, une authentification en temps réel de l'utilisateur de destination pourra être nécessaire.

8) Le fournisseur de service B envoie une réponse assertant l'identité de l'utilisateur de destination.

9) Le fournisseur de service A envoie à l'utilisateur ETS une réponse (par exemple affichage web visuel) validant l'identité de l'utilisateur de destination de la session de communication ETS.

Les utilisateurs ETS sont de plus en plus amenés à utiliser des services de données (par exemple messagerie électronique, messagerie instantanée et messagerie textuelle). Dans certaines situations, il pourra être nécessaire d'authentifier ou de valider les sources de ces services de données. Compte tenu de l'abondance des courriers poubelle et des spams, il sera essentiel pour les utilisateurs ETS de pouvoir distinguer et valider les messages authentiques pendant certaines catastrophes.

La Figure III.5 illustre un exemple de cas d'utilisation relatif à l'assertion de la source d'un message textuel. Dans cet exemple, on suppose que l'utilisateur ETS reçoit un message textuel provenant d'une source qui peut éventuellement être un autre utilisateur ETS. Pour obtenir la garantie de la source du message textuel, il est fait appel aux services d'identité d'un fournisseur de service. Le service d'identité utilisé pour l'assertion de la source du message textuel peut éventuellement faire partie du service de messagerie textuelle proprement dit.



NOTE – Dans un souci de simplicité, les flux de signalisation et les interactions ne sont pas tous représentés.

Figure III.5 – Assertion de la source d'un message textuel

Les interactions sont résumées ci-après:

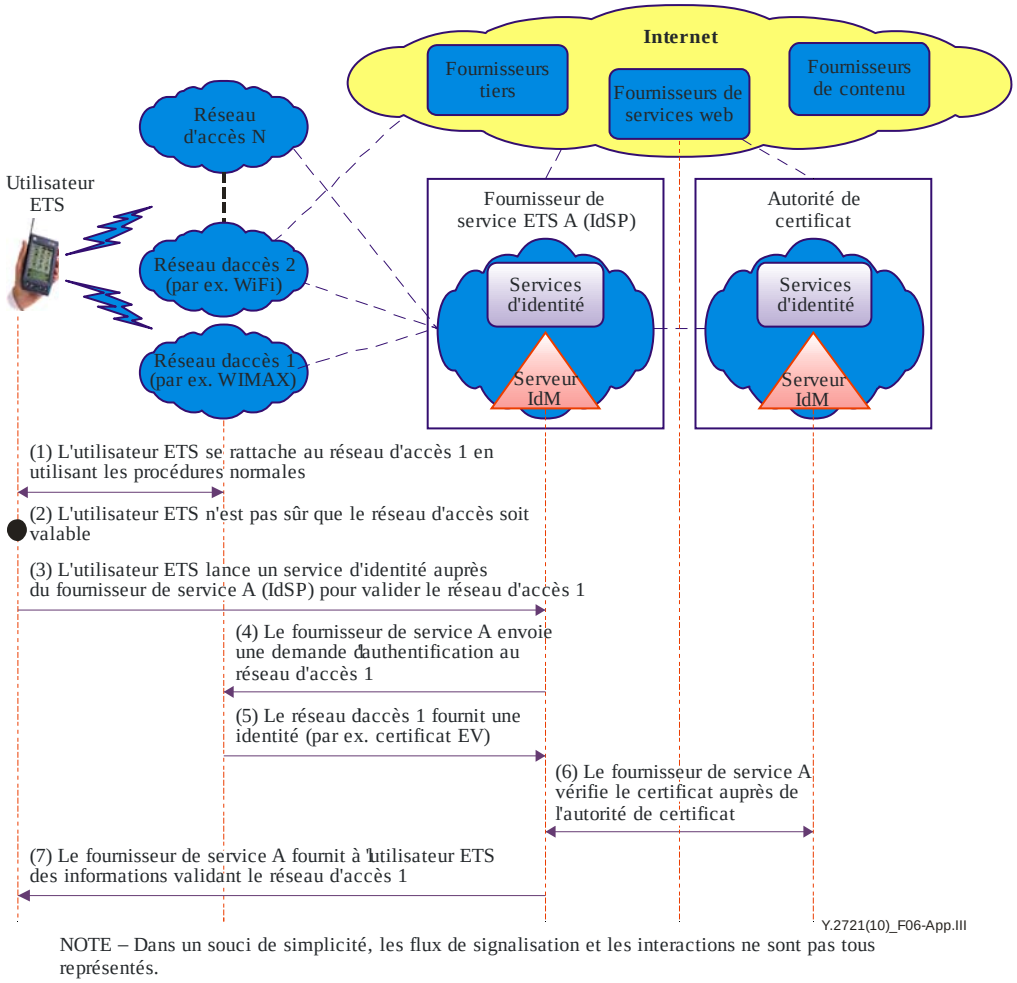
1) L'utilisateur ETS reçoit un message textuel.
2) L'utilisateur ETS souhaite vérifier l'authenticité de la source du message textuel et lance un service d'identité auprès du fournisseur de service A.
3) L'utilisateur ETS reçoit un défi d'authentification.
4) L'utilisateur ETS fournit les justificatifs pour l'authentification.
5) Le fournisseur de service A authentifie l'utilisateur ETS et vérifie qu'il est autorisé à utiliser le service d'identité.
6) Le fournisseur de service A envoie au fournisseur de service B une demande d'assertion de la source du message textuel.
7) Le fournisseur de service B traite la demande et vérifie la source du message textuel. Pour cela, une interaction avec la source du message textuel peut être nécessaire.
8) Le fournisseur de service B envoie au fournisseur de service A une réponse assertant l'identité de la source du message textuel.
9) Le fournisseur de service A envoie à l'utilisateur ETS des informations validant la source du message textuel.

III.5 Identification et authentification fiables des fournisseurs de service dans un environnement multifournisseur

L'infrastructure de communication actuelle a évolué vers un environnement qui comporte de multiples fournisseurs: fournisseurs d'accès fixe et mobile utilisant différentes technologies (par exemple xDSL, câble, FTTX, WiFi, WiMAX, EV-DO, LTE), fournisseurs de services de communications utilisant des "réseaux IP centraux gérés", fournisseurs de services web, fournisseurs de contenu et fournisseurs tiers. Dans cet environnement multifournisseur, on ne peut plus se fier implicitement à l'identité du fournisseur de service, comme c'était le cas dans l'environnement fermé du RTPC.

L'environnement multifournisseur ouvert nécessite des capacités permettant d'identifier, d'authentifier et d'autoriser de façon fiable les fournisseurs de service, faute de quoi des entités illégitimes risquent d'usurper ou de falsifier l'identité de fournisseurs de service légitimes ou de les représenter de manière inexacte. Des capacités de gestion IdM permettant d'identifier et de valider les fournisseurs de service sont donc essentielles pour la protection de l'infrastructure. Lorsque les fournisseurs de service prennent en charge des services ETS, ces capacités sont essentielles pour la sécurité nationale.

La Figure III.6 montre un exemple de cas d'utilisation du service ETS dans lequel l'utilisateur ETS tente d'obtenir un accès au réseau dans un environnement multifournisseur. Plus précisément, l'utilisateur ETS est en itinérance et a la possibilité de rattacher son combiné mobile à l'un des fournisseurs de réseau d'accès offrant des services dans la zone (il est possible que les fournisseurs de service ne soient pas tous des fournisseurs de service ETS autorisés). Dans cet exemple de cas d'utilisation, on suppose que l'utilisateur ETS se rattache au réseau d'accès 1 en premier choix. Après son rattachement, l'utilisateur ETS souhaite valider le réseau avant d'engager des communications ETS sensibles. Pour valider le fournisseur de réseau d'accès, il existe plusieurs possibilités et variantes, notamment une authentification directe par l'utilisateur ETS. On suppose dans cet exemple que l'utilisateur ETS utilise les services d'identité du fournisseur de service ETS A pour valider le réseau d'accès. Dans cet exemple, l'utilisateur ETS fait confiance au fournisseur de service A et accepte les informations de validation envoyées par ce fournisseur au sujet du réseau d'accès 1.



NOTE – Dans un souci de simplicité, les flux de signalisation et les interactions ne sont pas tous représentés.

Figure III.6 – Validation du fournisseur de service d'accès

Les interactions sont résumées ci-après:

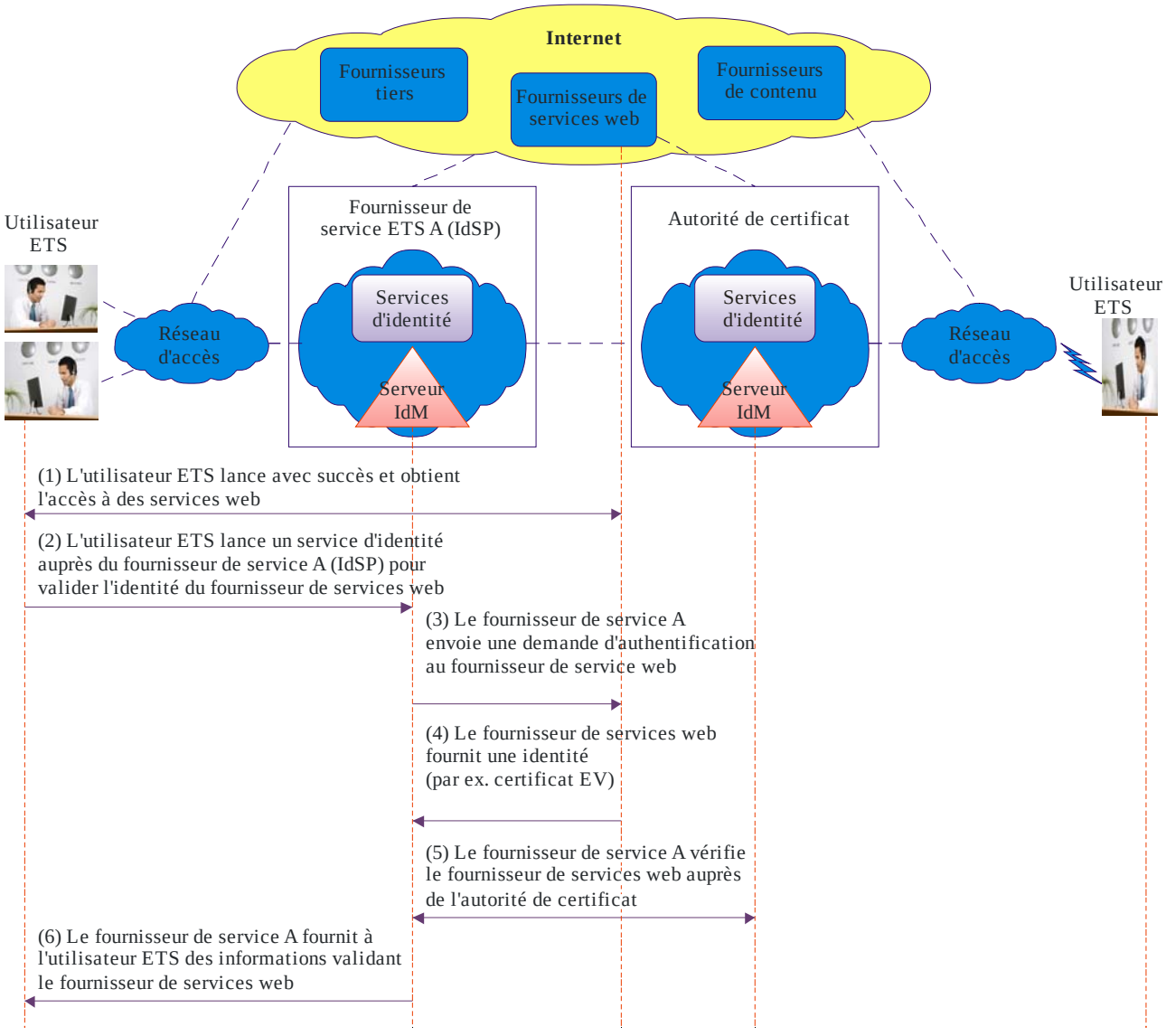
1) L'utilisateur ETS est en itinérance avec un combiné mobile qu'il peut rattacher à plusieurs types de réseau d'accès (par exemple WiFi, WIMAX, LTE ou EV-DO). L'utilisateur ETS rattache son combiné mobile au réseau 1 (il s'agit du premier choix basé sur des facteurs comme les fournisseurs ETS connus et l'intensité du signal).
2) L'utilisateur ETS souhaite valider le réseau 1 avant d'autoriser des services.
3) L'utilisateur ETS lance un service d'identité auprès du fournisseur de service ETS A pour valider le réseau d'accès 1.
4) Le fournisseur de service A envoie une demande d'authentification au réseau d'accès 1.
5) Le réseau d'accès 1 fournit des informations d'identité pour l'authentification (par exemple certificat UIT-T X.509 de validation étendue).
6) Le fournisseur de service ETS A vérifie le certificat du réseau 1 auprès de l'autorité de certificat.
7) Le fournisseur de service ETS A fournit à l'utilisateur ETS des informations validant le réseau d'accès 1.

Ainsi, l'utilisateur ETS peut continuer en étant assuré que son combiné mobile est rattaché à un réseau d'accès autorisé.

Après avoir obtenu un accès au réseau, l'utilisateur ETS est susceptible d'utiliser les services de plusieurs fournisseurs de service dans l'infrastructure multifournisseur. Par exemple, l'utilisateur ETS peut avoir besoin d'utiliser les services de fournisseurs de services web (par

exemple fournisseurs de données terrestres et d'autres données de cartographie) ou de fournisseurs de contenu (par exemple fournisseurs de service offrant une transmission en continu en temps réel depuis une caméra de surveillance ou des vidéos ou des rapports météorologiques). L'utilisateur ETS peut accéder aux services de fournisseurs de services web et de fournisseurs de contenu directement depuis un accès Internet ou indirectement par le biais des services de fournisseurs NGN. Quoi qu'il en soit, l'utilisateur ETS peut avoir besoin de valider le fournisseur d'un service spécifique.

La Figure III.7 illustre un exemple de cas d'utilisation dans lequel l'utilisateur ETS a besoin de valider l'identité d'un fournisseur de services web. Comme dans le cas d'utilisation ci-dessus, pour valider le fournisseur de services web, il existe de nombreuses possibilités et variantes, notamment une authentification directe par l'utilisateur ETS. Dans cet exemple, on suppose que l'utilisateur ETS utilise les services d'identité du fournisseur de service ETS A pour valider le fournisseur de services web. Comme dans l'exemple précédent, l'utilisateur ETS fait confiance au fournisseur de service A et accepte les informations de validation envoyées par ce fournisseur au sujet du fournisseur de services web.



NOTE – Dans un souci de simplicité, les flux de signalisation et les interactions ne sont pas tous représentés.

Figure III.7 – Validation d'un fournisseur de services web ou d'un fournisseur de contenu

Les interactions sont résumées ci-après:

1) L'utilisateur ETS lance avec succès et obtient l'accès à des services web. Toutefois, il souhaite valider le fournisseur de services web pour avoir confiance dans les données.

2) L'utilisateur ETS lance un service d'identité auprès du fournisseur de service ETS A pour valider le fournisseur de services web.

3) Le fournisseur de service ETS A envoie une demande d'authentification au fournisseur de services web.

4) Le fournisseur de services web fournit des informations pour l'authentification (par exemple certificat EV[1]).

5) Le fournisseur de service ETS A vérifie les informations auprès de l'autorité de certificat.

6) Le fournisseur de service ETS A fournit à l'utilisateur ETS des informations validant l'identité du fournisseur de services web.

La validation du fournisseur de services web permet à l'utilisateur ETS d'avoir confiance dans l'identité des services web et, par là-même, d'avoir confiance dans les informations obtenues à partir des services web.

III.6 Authentification unique et déconnexion unique

Les utilisateurs doivent généralement s'authentifier auprès à plusieurs systèmes hébergeant des services d'application (par exemple VoIP, données et vidéo), ce qui nécessite un nombre équivalent de dialogues d'authentification, dans chacun desquels les noms d'utilisateur et les informations d'authentification nécessaires peuvent être différents. Les administrateurs de système doivent gérer de façon coordonnée les comptes d'utilisateur dans chacun de ces multiples systèmes afin d'appliquer la politique de sécurité.

Les utilisateurs ETS pourront avoir besoin de tirer parti de capacités de gestion IdM du type "authentification/déconnexion uniques". Le principe de l'"authentification unique" est qu'un utilisateur final, un dispositif ou une combinaison utilisateur final et dispositif peut, grâce à une seule authentification (en fournissant des données de justificatifs pour l'authentification et l'autorisation) pour un service, être ensuite authentifié pour un ou plusieurs autres services dans le même domaine NGN ou, dans le cas de services fédérés, à travers plusieurs domaines NGN. L'intérêt de l'authentification unique est que l'utilisateur final n'a pas à s'authentifier pour chaque service. Le terme "authentification" employé ici correspond aux termes anglais "sign-on", "register with", "log-on" ou "log-in". De même, la "déconnexion unique" permet une déconnexion complète de plusieurs services d'application dans une session donnée.

Parmi les avantages potentiels des capacités d'authentification/déconnexion uniques pour les utilisateurs ETS, on peut citer:

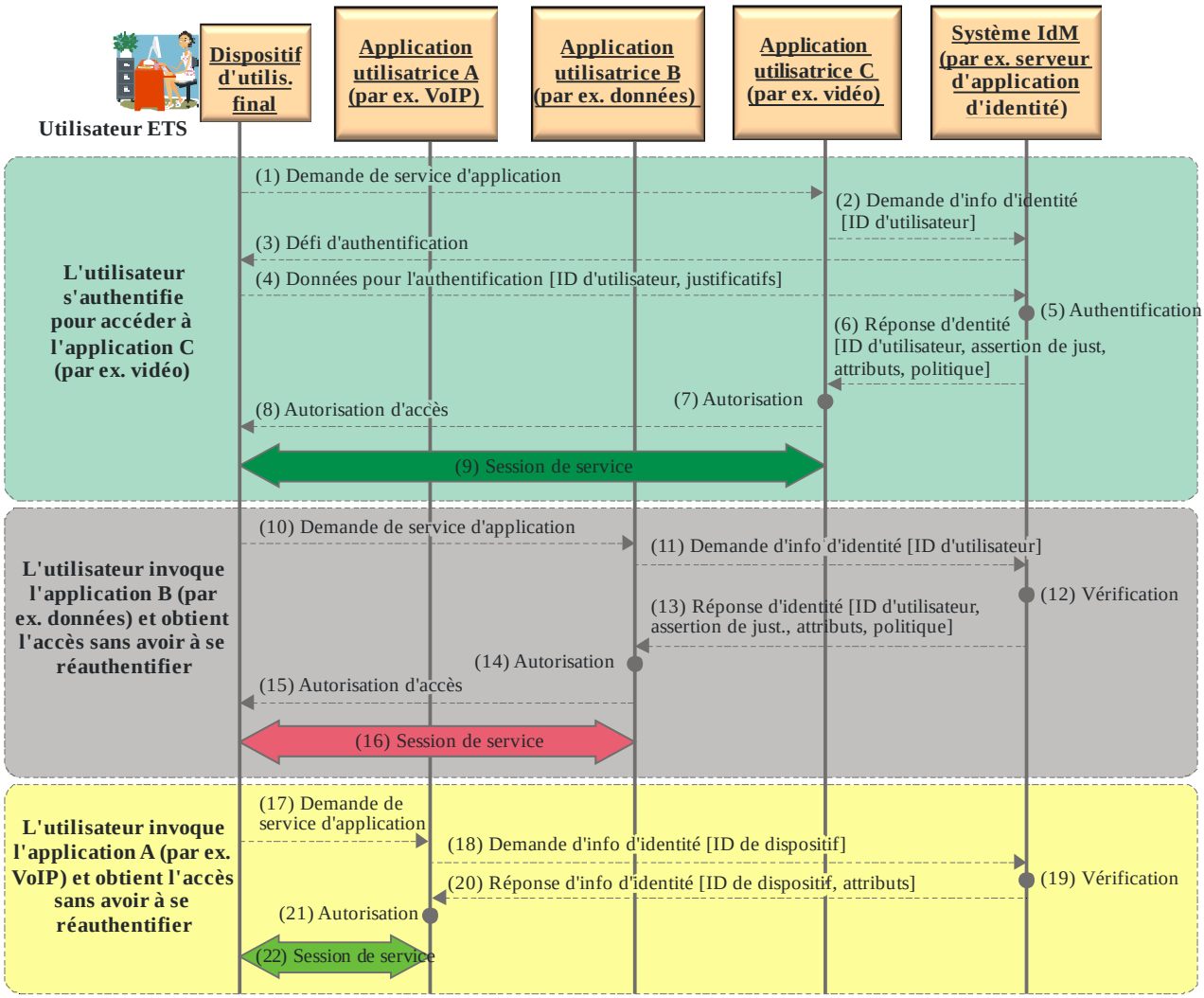
- Réduction du temps passé par les utilisateurs dans les opérations d'authentification auprès de différents domaines, et réduction du nombre d'échecs d'authentification. Amélioration de la sécurité du fait que l'utilisateur a besoin de traiter et de mémoriser un moins grand nombre d'informations d'authentification.
- Réduction du temps passé par les administrateurs de système à ajouter et supprimer des utilisateurs dans le système ou à modifier leurs droits d'accès.
- Amélioration de la sécurité du fait que les administrateurs de système sont davantage en mesure de maintenir l'intégrité de la configuration des comptes d'utilisateur et notamment

[1] Le certificat de validation étendue est un type spécial de certificat UIT-T X.509 qui nécessite une investigation approfondie au sujet de l'entité requérante par l'autorité de certificat avant d'être délivré.

en mesure d'interdire ou de supprimer l'accès d'un utilisateur individuel à toutes les ressources du système de manière coordonnée et cohérente.

La Figure III.8 illustre un exemple de cas d'utilisation relatif à l'utilisation d'un système de gestion IdM pour la prise en charge de l'"authentification unique/déconnexion unique" pour plusieurs services d'application (par exemple VoIP, données et vidéo) à l'intérieur du domaine d'un fournisseur NGN. Dans ce cas d'utilisation, des interactions existent entre les entités suivantes:

- Utilisateur final (utilisateur final et/ou dispositif d'utilisateur final).
- Système utilisateur (service d'application ou système de réseau).
- Système de gestion IdM (système de réseau fournissant des services de gestion IdM tels que l'enregistrement, l'authentification et l'autorisation, et des informations relatives au profil d'abonnement).



NOTE – Dans un souci de simplicité, les flux de signalisation et les interactions ne sont pas tous représentés.

Figure III.8 – Authentification unique

Dans cet exemple, on suppose que l'enregistrement du dispositif d'utilisateur final et son rattachement au réseau NGN se font selon les procédures normales.

Les flux d'appel sont les suivants:

1) Demande de service d'application: ce flux d'informations représente l'invocation du service d'application C (vidéo) par l'utilisateur final ETS.

2) Demande d'informations d'identité [ID d'utilisateur]: le service d'application C (vidéo) envoie une demande au système de gestion IdM en vue de l'assertion de l'identité de l'utilisateur et de la fourniture d'attributs associés à l'identité de l'utilisateur, qui peuvent notamment inclure des informations comme le profil de service, les privilèges, les préférences et des informations relatives aux politiques, par exemple toute politique ou restriction associée à l'identité.

3) Défi d'authentification: le système de gestion IdM envoie à l'utilisateur un défi d'authentification.

4) Données pour l'authentification [justificatifs]: l'utilisateur fournit des informations pour l'authentification (par exemple identité d'utilisateur et mot de passe ou numéro d'identification personnel).

5) Authentification: le système de gestion IdM procède à l'authentification et obtient les autres informations nécessaires, par exemple des informations provenant d'autres systèmes de réseau (serveur HSS ou autre base de données d'abonnement par exemple).

6) Réponse d'identité [assertions de justificatifs, attributs, politique]: le système de gestion IdM fournit des informations assertant les justificatifs. Parmi les autres informations pouvant être incluses, on peut citer les attributs associés à l'identité de l'utilisateur (par exemple privilèges et préférences) et la politique associée aux informations d'identité (par exemple toute restriction concernant l'utilisation, l'affichage et la diffusion).

7) Autorisation: après avoir traité les informations, le service d'application C (vidéo) détermine que l'utilisateur est autorisé à utiliser le service.

8) Autorisation d'accès: le service d'application C (vidéo) indique à l'utilisateur que l'accès au service est autorisé.

9) Session de service: la session de l'utilisateur avec le service d'application C (vidéo) est établie avec succès.

10) Demande de service d'application: l'utilisateur invoque le service d'application B (données).

11) Demande d'informations d'identité [ID d'utilisateur]: le service d'application B (données) envoie une demande au système de gestion IdM en vue de l'assertion de l'identité de l'utilisateur et de la fourniture d'attributs associés à l'identité de l'utilisateur, qui peuvent notamment inclure des informations comme le profil de service, les privilèges, les préférences et des informations relatives aux politiques, par exemple toute politique ou restriction associée à l'identité.

12) Vérification: le système de gestion IdM traite la demande, détermine que l'authentification unique s'applique et vérifie que l'authentification de l'utilisateur est toujours valable.

13) Réponse d'informations d'identité [assertions de justificatifs, attributs, politique]: le système de gestion IdM fournit des informations assertant les justificatifs. Parmi les autres informations pouvant être incluses, on peut citer les attributs associés à l'identité de l'utilisateur (par exemple privilèges et préférences) et la politique associée aux informations d'identité (par exemple toute restriction concernant l'utilisation, l'affichage et la diffusion).

14) Autorisation: après avoir traité les informations, le service d'application B (données) détermine que l'utilisateur est autorisé à utiliser le service.

15) Autorisation d'accès: le service d'application B (données) indique à l'utilisateur que l'accès au service est autorisé.

16) Session de service: la session de l'utilisateur avec le service d'application B (données) est lancée avec succès.

17) Demande de service d'application: l'utilisateur invoque le service d'application A (VoIP).

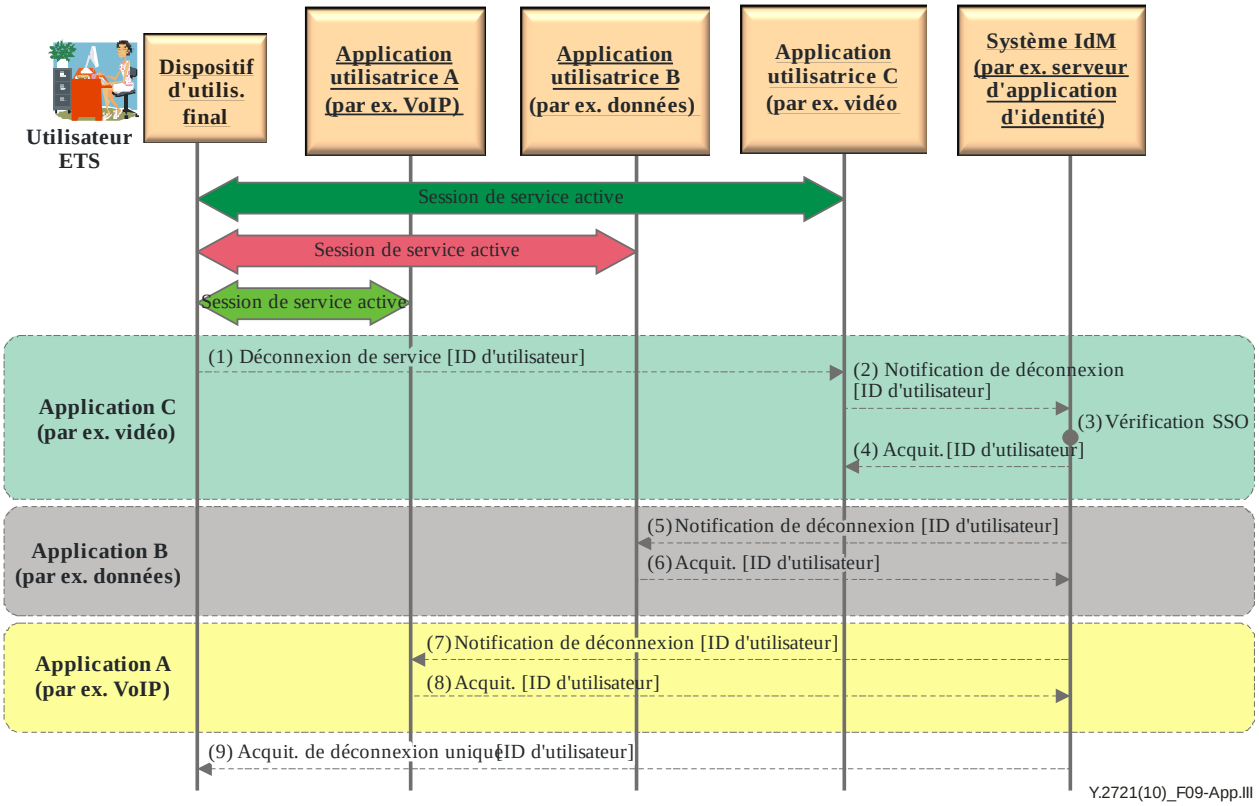
18) Demande d'informations d'identité [ID de dispositif]: le service d'application A (VoIP) envoie une demande au système de gestion IdM en vue de l'assertion de l'identité de l'utilisateur et de la fourniture d'attributs associés à l'identité du dispositif.

19) Vérification: le système de gestion IdM traite la demande, détermine que l'authentification unique s'applique et vérifie que l'authentification de l'utilisateur est toujours valable.

20) Réponse d'informations d'identité [assertions de justificatifs, attributs, politique]: le système de gestion IdM fournit des informations assertant les justificatifs. Parmi les autres informations pouvant être incluses, on peut citer les attributs associés à l'identité du dispositif (par exemple privilèges et préférences) et la politique associée aux informations d'identité (par exemple toute restriction concernant l'utilisation, l'affichage et la diffusion).

21) Autorisation: après avoir traité les informations, le service d'application A (VoIP) détermine que l'utilisateur est autorisé à utiliser le service.

22) Session de service d'application: l'utilisateur établit une session avec le service d'application A (VoIP).



NOTE – Dans un souci de simplicité, les flux de signalisation et les interactions ne sont pas tous représentés.

Figure III.9 – Déconnexion unique

La Figure III.9 illustre le cas d'un service de "déconnexion unique" permettant à l'utilisateur de se déconnecter automatiquement de plusieurs services d'application (VoIP, données et vidéo) sans avoir à se déconnecter de chaque service d'application dans la session. Dans ce cas d'utilisation, on suppose que l'utilisateur est dans une session de service avec les services d'application actifs A (VoIP), B (données) et C (vidéo).

Les flux d'appel sont les suivants:

1) Déconnexion de service [ID d'utilisateur]: l'utilisateur ETS demande qu'il soit mis fin à la session de service.

2) Notification de déconnexion [ID d'utilisateur]: le service d'application C (vidéo) informe le système de gestion IdM de la demande de déconnexion de l'utilisateur.

3) Vérification SSO: le système de gestion IdM détermine que la déconnexion unique s'applique et vérifie les services d'application actifs.

4) Acquittement [ID d'utilisateur]: le système de gestion IdM envoie un acquittement de fin de session de service au service d'application C (vidéo).

5) Notification de déconnexion [ID d'utilisateur]: le système de gestion IdM informe le service d'application B (données) de la déconnexion.

6) Acquittement [ID d'utilisateur]: le service d'application B (données) acquitte la déconnexion.

7) Notification de déconnexion [ID d'utilisateur]: le système de gestion IdM informe le service d'application A (VoIP) de la déconnexion.

8) Acquittement [ID d'utilisateur]: le service d'application A (VoIP) acquitte la déconnexion.

9) Acquittement de déconnexion unique [ID d'utilisateur]: le système de gestion IdM envoie un acquittement à l'utilisateur pour confirmer la déconnexion de tous les services d'application actifs dans la session.

Appendice IV

Cas d'utilisation liés au mobile

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

IV.1 Introduction

Le présent appendice contient des exemples de cas d'utilisation de la gestion IdM liés au mobile, qui sont fondés sur les cas d'utilisation décrits dans le livre blanc de 3G Americas intitulé *Identity Management: Overview of Standards and Technologies for Mobile and Fixed Internet* [b-3G Americas White Paper].

IV.2 Exemples de cas d'utilisation

IV.2.1 Un utilisateur mobile avec un dispositif 3G muni d'une carte UICC accède au portail d'un opérateur MNO (boutique web) pour acheter une sonnerie téléphonique.

Acteurs:

- Utilisateur mobile.
- Opérateur MNO (opérateur de réseau mobile).
- Le fournisseur de service est l'opérateur MNO.

Avantages pour l'utilisateur:

- Expérience d'authentification unique avec accès à différents services de l'opérateur MNO.

Principales contraintes:

- Le fournisseur de service et l'opérateur MNO sont dans le même cercle de confiance (Liberty Alliance).

IV.2.2 Un utilisateur mobile avec un dispositif 3G muni d'une carte UICC accède à la boutique web disponible sur le portail d'un opérateur MNO. Il navigue dans le catalogue de produits numériques figurant sur le portail, voit un produit faisant l'objet d'une promotion spéciale (par exemple un jeu vidéo pour lequel l'opérateur MNO dispose d'un accord exclusif de distribution du contenu) et l'achète, il décide ensuite de porter le montant à payer sur sa facture de téléphone mobile. L'utilisateur peut télécharger le jeu vidéo via un lien sécurisé redirigé de l'opérateur MNO vers le fournisseur de contenu.

Acteurs:

- Utilisateur mobile.
- Opérateur MNO.
- Le fournisseur de service a est l'opérateur MNO; le fournisseur de service b est le fournisseur de contenu externe (par exemple jeu vidéo).

Avantages pour l'utilisateur:

- Expérience d'authentification unique auprès d'un opérateur MNO et d'un fournisseur externe.
- Capacité d'utiliser ses justificatifs auprès de l'opérateur MNO pour mener à bien une transaction avec un fournisseur de contenu externe.

Principales contraintes:

- Le fournisseur de service a (opérateur MNO) et le fournisseur de service b (fournisseur de contenu fournissant le jeu vidéo) sont dans le même cercle de confiance.

IV.2.3 Alors qu'il est en itinérance dans un autre pays, un utilisateur mobile utilise son téléphone intelligent 3G muni d'une carte UICC. Tout en navigant sur l'Internet, il souscrit un abonnement payant à un magazine auto étranger et paye avec sa carte de crédit (certains attributs du profil de l'utilisateur conservé par l'opérateur MNO sont divulgués afin de pouvoir réaliser le processus de demande d'abonnement au magazine). Le paiement est autorisé par la société de carte de crédit pour le compte de l'utilisateur mobile sur le portail du magazine auto.

Acteurs:

- Utilisateur mobile.
- Opérateur MNO.
- Le fournisseur de service a est le fournisseur de contenu (magazine auto); le fournisseur de service b est la société de carte de crédit.

Avantages pour l'utilisateur:

- Expérience d'authentification unique auprès de l'opérateur MNO et de la société de carte de crédit.
- Capacité d'utiliser ses justificatifs auprès de l'opérateur MNO pour autoriser le paiement auprès de la société de carte de crédit afin de mener à bien une transaction avec un fournisseur de contenu externe.
- Capacité de réutiliser les attributs personnels du profil d'abonné MNO pour souscrire un abonnement à un service externe, ce qui évite de devoir saisir à nouveau un grand nombre de ces données.

Principales contraintes:

- L'opérateur MNO et le fournisseur de service b (société de carte de crédit) sont dans le même cercle de confiance.
- Le fournisseur de service a (fournisseur du magazine auto étranger) n'est pas dans le cercle de confiance.

IV.2.4 Alors qu'il est en itinérance dans un autre pays et attend dans un aéroport, un utilisateur mobile utilise son ordinateur portable 3G muni d'une carte UICC et souscrit au service WiFi de l'aéroport pour plusieurs heures. L'opérateur WLAN a conclu une alliance avec l'opérateur MNO de l'utilisateur mobile et peut donc accepter que l'utilisateur porte le montant à payer pour l'utilisation WiFi sur sa facture de téléphone mobile. Par ailleurs, tout en utilisant le service WiFi, l'utilisateur mobile accède à plusieurs portails web avec lesquels il interagit fréquemment, à savoir: le portail d'une banque, celui d'une agence de voyages et celui d'une société d'investissements financiers. L'utilisateur souhaite pouvoir utiliser les services offerts par ces sociétés sur le web sans avoir à se reconnecter et pouvoir aussi échanger des informations personnelles privées en toute sécurité.

Acteurs:

- Utilisateur mobile.
- Opérateur WLAN.
- Opérateur MNO.
- Le fournisseur de service a est l'opérateur MNO; le fournisseur de service b est la banque, le fournisseur de service c est l'agence de voyage et le fournisseur de service d est la société d'investissements financiers.

Avantages pour l'utilisateur:

- Expérience d'authentification unique auprès de l'opérateur MNO et de l'opérateur WiFi.
- Capacité d'utiliser ses justificatifs auprès de l'opérateur MNO pour autoriser le paiement du service WiFi.

- Capacité d'accéder à plusieurs fournisseurs de service sur le web non affiliés auprès de l'opérateur MNO avec des procédures de connexion simplifiées et de transférer en toute sécurité des informations privées.

Principales contraintes:

- L'opérateur MNO et l'opérateur WLAN sont dans le même cercle de confiance.
- Les fournisseurs de service b (banque), c (agence de voyage) et d (société d'investissements financiers) ne sont pas dans le même cercle de confiance.

IV.2.5 Un utilisateur mobile utilise son ordinateur portable 3G muni d'une carte UICC à la maison, il navigue sur l'Internet en utilisant son service DSL large bande résidentiel et accède au portail de son opérateur MNO. Il paye la facture de son compte de service mobile avec sa carte de crédit (une autorisation préalable est enregistrée) et ajoute une nouvelle option à son abonnement mobile. Il accède ensuite à un site de location de films, télécharge un film et paye avec sa carte de crédit (sans autorisation préalable).

Acteurs:

- Utilisateur mobile.
- Opérateur DSL de réseau fixe.
- Opérateur MNO.
- Le fournisseur de service a est l'opérateur MNO; le fournisseur de service b est le portail de location de films; le fournisseur de service c est la société de carte de crédit.

Avantages pour l'utilisateur:

- Expérience d'authentification unique auprès de l'opérateur de réseau fixe et de l'opérateur MNO.
- Capacité d'utiliser ses justificatifs auprès de l'opérateur de réseau fixe pour authentifier son compte de service mobile et commander des services MNO supplémentaires.
- Capacité d'autoriser le paiement de l'achat de contenu auprès d'un fournisseur de service externe (par exemple société de location de films) avec sa carte de crédit.

Principales contraintes:

- L'opérateur MNO, l'opérateur de réseau fixe et le fournisseur de service c (société de carte de crédit) sont dans le même cercle de confiance.
- Le fournisseur de service b (location de films) n'est pas dans le même cercle de confiance.

IV.2.6 Un utilisateur mobile avec un dispositif 3G muni d'une carte UICC souhaite accéder à des ressources (par exemple service d'annuaire d'entreprise) situées dans un réseau d'entreprise.

Acteurs:

- Utilisateur mobile.
- Opérateur MNO.
- Système de gestion IdM d'entreprise.
- Serveur de services d'annuaire d'entreprise (serveur EDS).

Les interactions de haut niveau entre ces acteurs sont décrites ci-dessous. L'utilisateur mobile demande un service au serveur EDS.

- Le serveur EDS demande à l'utilisateur de s'authentifier.
- L'utilisateur, qui a été authentifié par le système MNO, obtient de ce système des justificatifs pour l'authentification par le système de gestion IdM d'entreprise.

- L'utilisateur soumet les justificatifs au système de gestion IdM d'entreprise et, une fois que l'authentification a abouti, obtient de ce système des justificatifs pour l'authentification auprès du serveur EDS.
- L'utilisateur répond à la demande du serveur EDS en fournissant les justificatifs reçus du système de gestion IdM d'entreprise.
- L'utilisateur authentifié obtient le service qu'il a demandé au serveur EDS.

Avantages pour l'utilisateur:

- L'utilisateur mobile peut accéder effectivement aux ressources disponibles dans son réseau d'entreprise (par exemple service d'annuaire d'entreprise) tout en respectant les exigences de sécurité strictes généralement imposées par les environnements informatiques des entreprises.

Principales contraintes:

- Une authentification à deux facteurs (par exemple ID d'utilisateur/mot de passe/PIN) peut être requise par le système de gestion IdM d'entreprise en plus des justificatifs fournis à l'utilisateur par l'opérateur MNO.
- Les systèmes de gestion IdM de l'opérateur MNO et de l'entreprise sont dans le même cercle de confiance.

Appendice V

Exemples de modèles de transaction IdM

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

V.1 Introduction

Le présent appendice donne des exemples de modèles de transaction IdM, qui sont décrits dans [b-UIT-T X.1250]. Des modèles autres que ceux qui sont inclus dans le présent appendice sont également possibles.

V.2 Exemples de modèles possibles de transactions en gestion d'identité

L'une des principales transactions en gestion d'identité correspond au processus de base question/réponse commun à la plupart des échanges d'information structurés illustré sur la Figure V.1. La forme la plus basique d'échange de messages fait intervenir deux parties utilisant un protocole et un modèle informationnel convenus.

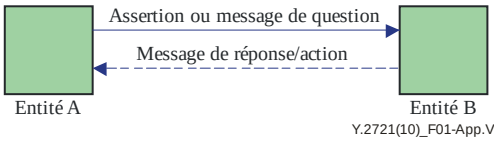


Figure V.1 – Processus de base de question/réponse pour l'échange d'informations

Les parties participant à ce processus peuvent être n'importe quel type d'entité. Une entité peut être une personne physique, un animal, une personne morale, une organisation, une chose active ou passive, un dispositif, une application logicielle, un service, etc., ou un groupe de ces éléments. Dans le contexte des télécommunications, il peut s'agir de points d'accès, d'abonnés, d'utilisateurs, d'éléments de réseau, de réseaux, d'applications logicielles, de services et de dispositifs, d'interfaces, etc. Il peut s'agir de n'importe quel objet physique ou virtuel, tel qu'un équipement de réseau, un logiciel, des dispositifs terminaux, des capteurs, des objets physiques activement étiquetés (par exemple, utilisant des RFID ou des codes optiques) ou des objets passivement étiquetés. Des dispositifs de réseau peuvent, par exemple, être traités comme des entités sous réserve de capacités spéciales de gestion IdM pour le compte d'utilisateurs finals, de fournisseurs et d'autorités publiques. Dans le contexte de la gestion des droits numériques, l'entité peut être un élément protégé par les droits de la propriété intellectuelle ou les droits d'auteur, tel qu'un contenu multimédia ou de TVIP. Un type particulier d'entité est le groupe. L'identité du groupe correspond à l'intersection des identités (attributs communs) de ses membres.

La plupart des cas d'utilisation de la gestion d'identité font appel à des modèles complexes. Par exemple, lorsque la partie utilisatrice qui reçoit à l'origine la déclaration n'est pas le fournisseur de service d'identité (voir les Figures V.2 et V.3), la fonction de fournisseur de service d'identité est séparée et distincte de celle de la partie utilisatrice; la partie utilisatrice évalue les réponses données par le ou les fournisseurs de service d'identité et décide s'il existe un degré suffisant de garantie d'authentification d'entité. La principale fonction d'un fournisseur de service d'identité est de gérer la création, la mise à jour, la vérification, la suspension et la suppression d'informations d'identité.

Il existe de nombreux modèles possibles d'échange d'informations d'identité. Un modèle couramment utilisé est le modèle tripartite avec question/réponse illustré sur la Figure V.2. Certains des nouveaux protocoles de gestion IdM "ouverts" sont fondés sur ce modèle.

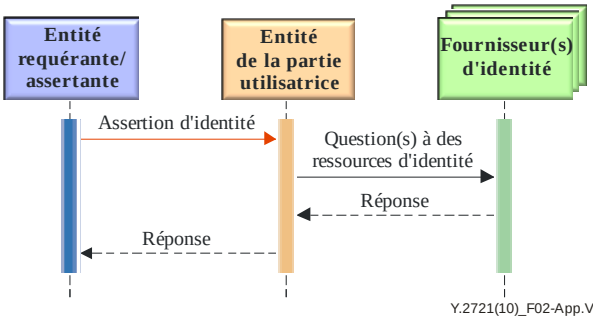


Figure V.2 – Exemple d'un modèle tripartite de gestion d'identité

Un autre modèle de gestion d'identité, qui donne à l'entité requérante plus de pouvoir dans les relations d'identité, est illustré sur la Figure V.3.

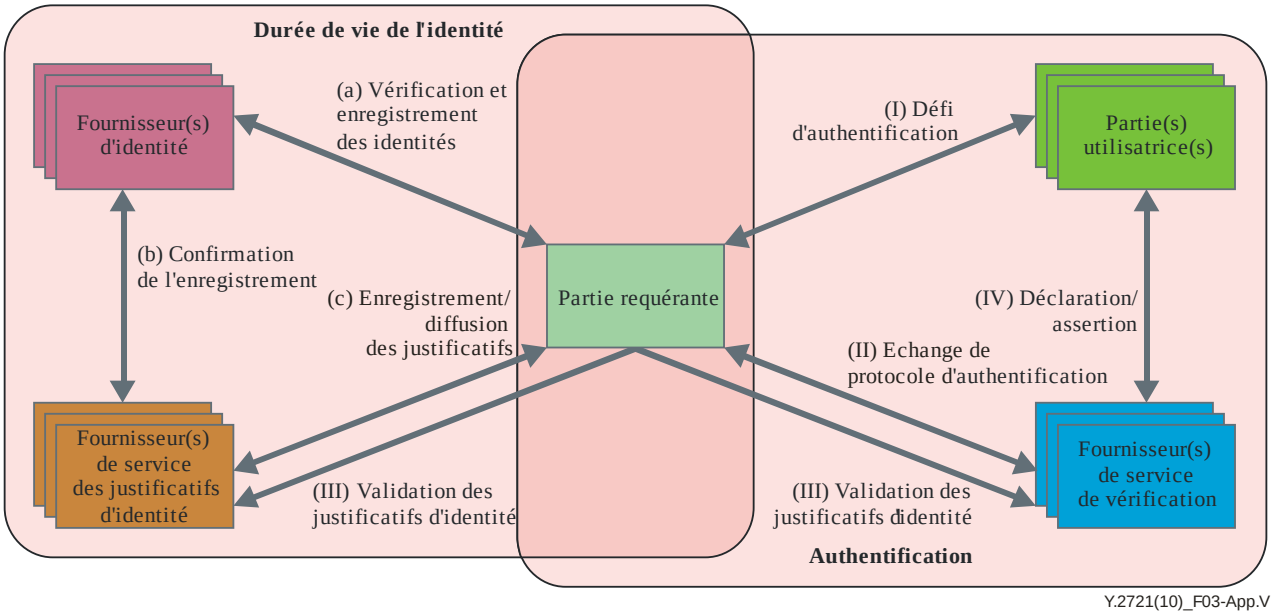


Figure V.3 – Exemple d'un modèle de gestion d'identité à cinq parties centré sur l'utilisateur

Les modèles "centrés sur l'utilisateur" (c'est-à-dire dans lesquels les parties requérantes doivent pouvoir exercer un contrôle total sur l'utilisation de leurs identités) font l'objet d'une importante attention et peuvent en outre être rendus obligatoires dans des juridictions nationales et régionales. La Figure V.3 montre un exemple où les rôles spécialisés et capacités de gestion d'identité sont fournis par différents fournisseurs de service. Toutes les questions/réponses passent par la partie requérante. Dans ces types de modèle, les entités sont définies de la façon suivante:

- Fournisseur d'identité: entité qui maintient, gère et peut créer des informations d'identités fiables concernant d'autres entités (par exemple, utilisateurs finals, organisations et dispositifs) et offre des services fondés sur l'identité. Cette entité, chargée de l'attribution et de la diffusion d'attributs (par exemple, pour un abonné à un fournisseur de justificatifs d'identité), lesquels constituent l'identité dans un contexte spécifique – on parle aussi d'inscription – est responsable de la gestion de l'identité, pendant toute sa durée de vie, ce qui comprend les activités de vérification, enregistrement et maintenance de l'identité, mais également sa révocation.

- Fournisseur de service des justificatifs d'identité: entité fournissant les capacités relatives à la diffusion des justificatifs d'identité et des jetons (par exemple, justificatifs liant des jetons à des identificateurs et attributs vérifiables).
- Fournisseur de service de vérification: entité fournissant des capacités d'évaluation des informations d'identité (par exemple, déclarations et justificatifs d'identité) et de classification de leur validité.
- Partie utilisatrice [UIT-T Y.2720]: entité qui est tributaire d'une représentation ou d'une déclaration d'identité soumise par une entité requérante/assertante dans un contexte de demande donné.

Appendice VI

Exemple de scénario de déploiement de la gestion IdM dans un réseau NGN

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

VI.1 Introduction

Le présent appendice décrit un exemple de scénario de déploiement de la gestion IdM dans un réseau NGN.

VI.2 Déploiement de l'architecture de gestion IdM

Dans un réseau NGN, on peut déployer une infrastructure de gestion IdM avec des capacités permettant de prendre en charge des services fondés sur l'identité pour les utilisateurs, sur la base des capacités de services web et des spécifications définies par le Liberty Alliance Project et OpenID, par exemple des capacités de gestion IdM permettant aux utilisateurs d'accéder à des services parmi différents fournisseurs de service et d'application, y compris des services d'application fédérés. En outre, le réseau NGN peut prendre en charge des capacités de gestion IdM permettant d'offrir des services de fournisseur IdSP à d'autres fournisseurs d'application et de service (par exemple assertion de l'identité du dispositif d'un utilisateur et authentification, emplacement et autres informations liées à l'identité).

La prise en charge de capacités de gestion IdM permettant d'offrir des services IdSP ou de s'associer à d'autres fournisseurs d'application et de service qui utilisent différents types de systèmes de gestion IdM basés sur plusieurs sémantiques, schémas, mécanismes et technologies nécessitera des fonctions de relais et d'interfonctionnement appropriées pour faciliter l'interopérabilité. Par exemple, pour la prise en charge d'un service et de capacités de gestion IdM avec d'autres fournisseurs d'application et de service (par exemple fournisseurs de services web et fournisseurs de contenu), le réseau NGN pourrait prendre en charge:

- des capacités d'interfonctionnement de l'architecture GBA 3GPP avec le Liberty Alliance Framework;
- des capacités d'interfonctionnement de l'architecture GBA 3GPP avec OpenID;
- d'autres mécanismes d'interfonctionnement avec OpenID et le Liberty Alliance Framework.

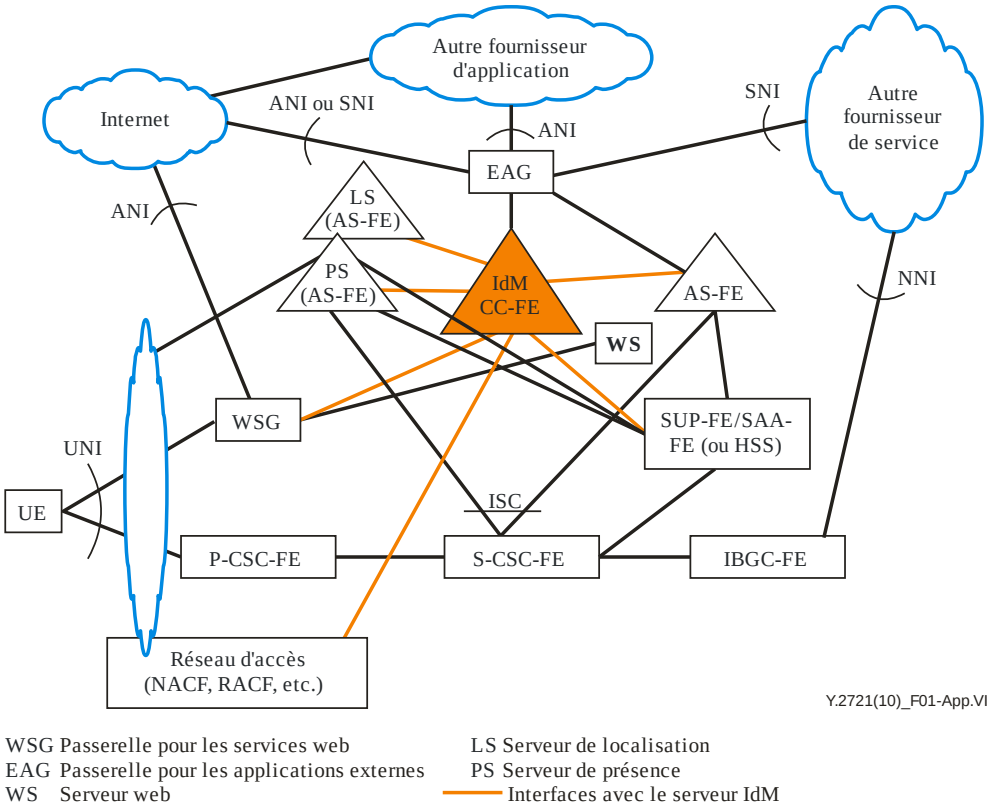


Figure VI.1 – Exemple de déploiement de la gestion IdM dans un réseau NGN

La Figure VI.1 illustre un exemple de déploiement de la gestion IdM dans un réseau NGN. Cet exemple montre l'utilisation d'un serveur de gestion IdM qui peut être un tout autonome ou un ensemble de fonctions qui sont réparties et/ou situées dans le serveur HSS. Le serveur de gestion IdM s'interface et interagit avec des éléments de réseau prenant en charge les entités fonctionnelles définies pour le réseau NGN. Il peut par exemple s'interfacer avec:

- des serveurs d'application (AS), tels que le serveur de localisation (LS) ou le serveur de présence (PS), ou d'autres applications afin de fournir un niveau élevé de garantie d'authentification et de prendre en charge des services d'application fondés sur l'identité;
- des serveurs de politique et de commande de rattachement au réseau pour la garantie d'authentification et la gestion de politique.

NOTE – Dans le cadre de certaines réglementations nationales, il pourra être nécessaire de mettre en œuvre des fonctions de gestion IdM distinctes dans les différentes strates des réseaux NGN.

Afin de prendre en charge certains services de gestion IdM pour les utilisateurs/abonnés et d'offrir des services IdSP ou de s'associer à d'autres fournisseurs d'application et de service, il faudra que le réseau NGN prenne en charge des capacités spécifiques pour contrôler l'accès et les échanges IdM avec d'autres fournisseurs d'application et de service (par exemple fournisseurs de services web et fournisseurs de contenu). Cet exemple donné à titre d'illustration montre l'utilisation d'une passerelle pour les services web (WSG) et d'une passerelle pour les applications externes (EAG) pour prendre en charge certains services de gestion IdM, avec la contribution d'autres fournisseurs d'application et de service ou avec l'association à de tels fournisseurs. Plus précisément, la Figure VI.1 montre le serveur de gestion IdM qui s'interface avec l'utilisateur via une passerelle pour les services web (WSG) qui authentifie l'utilisateur et lui fournit une interface pour gérer son profil d'identité. L'authentification mutuelle entre l'utilisateur et le fournisseur de service est également prise en charge, en fonction des besoins. Le serveur de gestion IdM s'interface aussi avec une passerelle pour les applications externes (EAG) qui permet à l'utilisateur d'accéder à des services basés sur le web dans le réseau NGN ou offerts par d'autres fournisseurs d'application ou de service.

Bibliographie

[b-UIT-T X.1141] Recommandation UIT-T X.1141 (2006), *Langage de balisage d'assertion de sécurité (SAML 2.0)*.

[b-UIT-T X.1250] Recommandation UIT-T X.1250 (2009), *Capacités de base pour l'amélioration de l'interopérabilité globale dans la gestion d'identité*.

[b-UIT-T X.1251] Recommandation UIT-T X.1251 (2009), *Cadre de contrôle de l'identité numérique par l'utilisateur*.

[b-UIT-T Y.2091] Recommandation UIT-T Y.2091 (2008), *Réseaux de prochaine génération: termes et définitions*.

[b-NIST SP 800-63] NIST Special Publication 800-63 (2006), *Electronic Authentication Guidelines*.

[b-NIST SP 800-94] NIST Special Publication 800-94 (2007), *Guide to Intrusion Detection and Prevention Systems (IDPS)*.

[b-CA/Browser Forum] CA/Browser Forum, *Guidelines For The Issuance And Management Of Extended Validation Certificates*.

[b-3G Americas White Paper] 3G Americas White Paper (2009), *Identity Management, Overview of Standards and Technologies for Mobile and Fixed Internet*.

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
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
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

Imprimé en Suisse
Genève, 2012