Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2720

(01/2009)

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

Réseaux de prochaine génération – Sécurité

Cadre de gestion d'identité des réseaux NGN

Recommandation UIT-T Y.2720

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 futurs	Y.2600–Y.2699
Sécurité	**Y.2700–Y.2799**
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999

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

Recommandation UIT-T Y.2720

Cadre de gestion d'identité des réseaux NGN

Résumé

La Recommandation UIT-T Y.2720 définit un cadre pour la gestion d'identité (IdM) dans les réseaux de prochaine génération (NGN). Ce cadre vise essentiellement à décrire une approche structurée permettant de concevoir, de définir et de mettre en œuvre des solutions IdM et de faciliter l'interopérabilité dans un environnement hétérogène.

La gestion des informations sur l'identité d'une entité (par exemple des identificateurs, des justificatifs d'identité et des attributs) n'est pas une question nouvelle, mais plus nous progressons vers un environnement de réseau intégré, dans lequel les services sont fondés sur des contextes et des rôles et peuvent être accessibles en tout lieu et en tout temps, plus la garantie, la sécurité et la gestion des informations d'identité deviennent complexes. Par ailleurs, les solutions retenues peuvent être différentes et indépendantes, d'où la nécessité d'assurer l'interopérabilité. En conséquence, il faut disposer de nouvelles fonctionnalités améliorées, automatisées et interopérables pour les raisons suivantes:

- les utilisateurs finals utilisent de plus en plus des identités multiples;
- ces identités peuvent être associées à des contextes et à des privilèges de service différents;
- il se peut que les identités n'identifient que partiellement l'utilisateur final;
- les identités peuvent être utilisées en tout temps et en tout lieu; et
- il se peut que les identités ne soient pas interopérables entre les fournisseurs.

La gestion IdM permet de remédier à cette situation et comporte un ensemble de fonctions et de fonctionnalités (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 d'identité, 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);
- permettre des applications commerciales et liées à la sécurité.

Ce cadre vise à servir de base à l'élaboration et à la définition de certains aspects de la gestion IdM, tels que les spécifications, les mécanismes et les procédures détaillés le cas échéant. Il donne également une vue d'ensemble claire et cohérente de l'intégralité de la gestion IdM dans le contexte des réseaux NGN.

Le cadre définit dans cette Recommandation est destiné aux réseaux NGN (c'est-à-dire aux réseaux gérés en mode paquet), tels que définis dans la Recommandation UIT-T Y.2001, *Aperçu général des réseaux de prochaine génération*. Il pourra cependant être appliqué, s'il y a lieu, à d'autres types de réseaux (par exemple les réseaux d'entreprise).

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

Source

La Recommandation UIT-T Y.2720 a été approuvée le 23 janvier 2009 par la Commission d'études 13 (2009-2012) de l'UIT-T selon la procédure définie dans la Résolution 1 de l'AMNT.

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 [avait/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.2720

Cadre de gestion d'identité des réseaux NGN

1 Domaine d'application

La présente Recommandation définit un cadre pour la gestion IdM dans les réseaux NGN. Elle vise essentiellement à décrire les concepts, les éléments fonctionnels et les fonctionnalités de base de la gestion d'identité qui peuvent être utilisés pour organiser et orienter des solutions structurées pour les réseaux NGN. La présente Recommandation vise à:

- décrire les motivations, les retombées et les avantages commerciaux des services de gestion IdM, ainsi que les fonctionnalités génériques utilisées pour garantir l'identité et définir les concepts de gestion IdM applicables aux réseaux NGN sur la base des prescriptions fonctionnelles et de l'architecture (FRA) de ces réseaux définies dans [b-UIT-T Y.2012], *Prescriptions fonctionnelles et architecture du réseau de prochaine génération version 1*;
- recenser et décrire les entités fonctionnelles, les rôles, les relations, les fonctions de validation et les communications prenant en charge les services et les fonctionnalités IdM pour les réseaux NGN;
- identifier et décrire les relations à l'intérieur d'un réseau pour la prise en charge de services et de fonctionnalités IdM dans un réseau NGN; et
- identifier et décrire les relations pour la prise en charge de services et de fonctionnalités IdM entre fournisseurs NGN (par exemple, à l'intérieur d'une fédération) et entre des fournisseurs NGN et d'autres fournisseurs (par exemple, entre fédérations).

Le cadre défini dans la présente Recommandation est destiné aux réseaux NGN (c'est-à-dire aux réseaux gérés en mode paquet), tels que définis dans [b-UIT-T Y.2001], *Aperçu général des réseaux de prochaine génération*, mais il pourra être appliqué, s'il y a lieu, à d'autres types de réseau (par exemple, les réseaux d'entreprise).

Il vise à servir de base à l'élaboration et à la définition de certains aspects de la gestion IdM pour les réseaux NGN, tels que les spécifications, les mécanismes et les procédures détaillés, le cas échéant. Il donne également une vue d'ensemble claire et cohérente de l'intégralité de la gestion IdM dans le contexte des réseaux NGN.

NOTE – Le terme "identité" employé dans la présente Recommandation 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.

2 Références

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

[UIT-T Y.2011] Recommandation UIT-T Y.2011 (2004), *Principes généraux et modèle de référence général pour les réseaux de prochaine génération*.

3 Définitions

3.1 Termes définis ailleurs

Les termes suivants, définis ailleurs, sont utilisés dans la présente Recommandation:

3.1.1 anonymat [b-UIT-T X.1121]: l'accès aux services est anonyme lorsqu'il n'est pas possible d'avoir accès aux données personnelles concernant l'utilisateur et son comportement – lieu de l'utilisateur, fréquence d'utilisation du service, etc.

3.1.2 authentification [b-UIT-T X.811]: attestation de l'identité revendiquée par une entité.

3.1.3 autorisation [b-UIT-T X.800]: attribution de droits, comprenant la permission d'accès sur la base de droits d'accès**.**

3.1.4 déclarant [b-UIT-T X.811]: entité qui est ou représente une entité principale à des fins d'authentification. Un déclarant comporte les fonctions nécessaires pour engager des échanges pour authentification au nom d'une entité principale.

3.1.5 délégation [b-UIT-T X.911]: action qui attribue une autorité, une responsabilité ou une fonction à un autre objet.

3.1.6 identificateur [b-UIT-T Y.2091]: 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).

3.1.7 réseau de prochaine génération (NGN) [b-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.

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

3.1.9 domaine sécurité [b-UIT-T X.810]: ensemble d'éléments, politique de sécurité, autorité de sécurité et ensemble d'activités liées à la sécurité dans lesquels l'ensemble des éléments est sujet à la politique de sécurité, pour les activités spécifiées et la politique de sécurité est administrée par l'autorité de sécurité, pour le domaine de sécurité.

3.1.10 vérificateur [b-UIT-T X.811]: entité qui est ou qui représente l'entité revendiquant une identité authentifiée. Un vérificateur comporte les fonctions nécessaires pour engager des échanges pour authentification.

3.2 Termes définis dans d'autres normes qui n'ont pas été élaborées par l'UIT

3.2.1 attribut [b-ETSI TS102 042]: information liée à une entité qui spécifie une caractéristique telle que la condition, la qualité ou d'autres informations associées à l'entité en question.

3.3 Termes définis dans la présente Recommandation

Les termes suivants sont définis dans la présente Recommandation:

3.3.1 garantie: niveau de confiance dans l'efficacité des caractéristiques et de l'architecture de sécurité des fonctionnalités de gestion d'identité établies pour assurer la mise en œuvre des politiques de sécurité conclues entre la partie utilisatrice et le fournisseur d'identité.

3.3.2 garantie d'authentification: voir garantie.

3.3.3 niveau de garantie: expression quantitative de la garantie convenue entre une partie utilisatrice et un fournisseur d'identité.

3.3.4 justificatif d'identité: objet identifiable qui peut être utilisé afin d'attester que le déclarant est ce qu'il revendique et de lui accorder des droits d'accès.

3.3.5 découverte: 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.

3.3.6 entité: tout type d'élément qui a une existence séparée et distincte et peut être identifié de manière unique. 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 systèmes. Une entité peut avoir plusieurs identificateurs.

3.3.7 fédération: création d'une relation entre deux entités ou plus ou association composée d'un nombre quelconque de fournisseurs de services et de fournisseurs d'identités.

3.3.8 identité fédérée: identité qui peut être utilisée pour accéder à un groupe de services ou d'applications défini selon les politiques et conditions d'une fédération.

3.3.9 identité: information sur une entité qui suffit à l'identifier dans un contexte donné.

3.3.10 fournisseur d'identités: entité qui crée, maintient et gère 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.

3.3.11 gestion d'identité: ensemble de fonctions et de fonctionnalités (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 d'identité, 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.

3.3.12 profil: expression structurée déduite du comportement d'une entité, favorisant ou permettant son identification; peut conclure la réputation de l'entité. Les profils peuvent être associés de manière univoque à une entité ou à une classe à laquelle l'entité est associée.

3.3.13 informations d'identification personnelle: informations relatives à une personne physique permettant de l'identifier (y compris les informations permettant d'identifier une personne lorsqu'elles sont combinées avec d'autres informations, même si elles n'identifient pas clairement la personne.

3.3.14 présence: ensemble d'attributs qui caractérisent une entité en relation avec le statut actuel.

3.3.15 respect de la vie privée: protection des informations d'identification personnelle.

3.3.16 partie utilisatrice: entité qui est tributaire d'une représentation ou d'une déclaration d'identité soumise par une entité requérante/assertante.

3.3.17 confiance: degré de fiabilité du caractère, de l'aptitude, du pouvoir ou de la vérité de quelqu'un ou de quelque chose.

4 Abréviations et acronymes

Les abréviations suivantes sont employées dans la présente Recommandation.

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

BSS système d'appui aux activités (*business support system*)

CSCF fonction de commande de session d'appel (*call session control function*)

FRA spécifications fonctionnelles et architecture (*functional requirements and architecture*)

GBA architecture d'amorçage générique (*generic bootstrapping architecture*)

IdM gestion d'identité (*identity management*)

IdP fournisseur d'identités (*identity provider*)

NGN réseaux de prochaine génération (*next generation networks*)

OAM&P exploitation, administration, maintenance et approvisionnement (*operation, administration, maintenance and provisioning*)

OSS système d'appui à l'exploitation (*operations support system*)

PII informations d'identification personnelle (*personally identifiable information*)

QoE qualité d'expérience (*quality of experience*)

QoS qualité de service (*quality of service*)

RP partie utilisatrice (*relying party*)

RTPC réseau téléphonique public commuté

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

SBC contrôleur de session en limite (*session border controller*)

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

SP fournisseur de services (*service provider*)

SS7 système de signalisation N° 7 (*signaling system No. 7*)

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

VoIP téléphonie utilisant le protocole Internet (*voice over Internet protocol*)

5 Introduction

5.1 Présentation de la gestion d'identité (IdM)

La gestion des informations sur l'identité d'une entité (par exemple des identificateurs, des justificatifs d'identité et des attributs) n'est pas une question nouvelle, mais plus nous progressons vers un environnement de réseau intégré, dans lequel les services sont fondés sur des contextes et des rôles et sont accessibles en tout lieu et en tout temps, plus la garantie, la sécurité et la gestion des informations d'identité deviennent complexes. Par ailleurs, les solutions retenues peuvent être différentes et indépendantes, d'où la nécessité d'assurer l'interopérabilité. En conséquence, il faut disposer de nouvelles fonctionnalités améliorées, automatisées et interopérables. Ce cadre vise essentiellement à décrire une approche structurée aux fins de la conception, de la définition et de la mise en œuvre de solutions qui facilitera l'interopérabilité dans un environnement hétérogène.

La gestion d'identité permet de remédier à cette situation et comporte un ensemble de fonctions et de fonctionnalités (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;
- garantir l'identité d'une entité; et
- permettre des applications commerciales et liées à la sécurité.

La Figure 1 donne un aperçu général de la gestion d'identité.

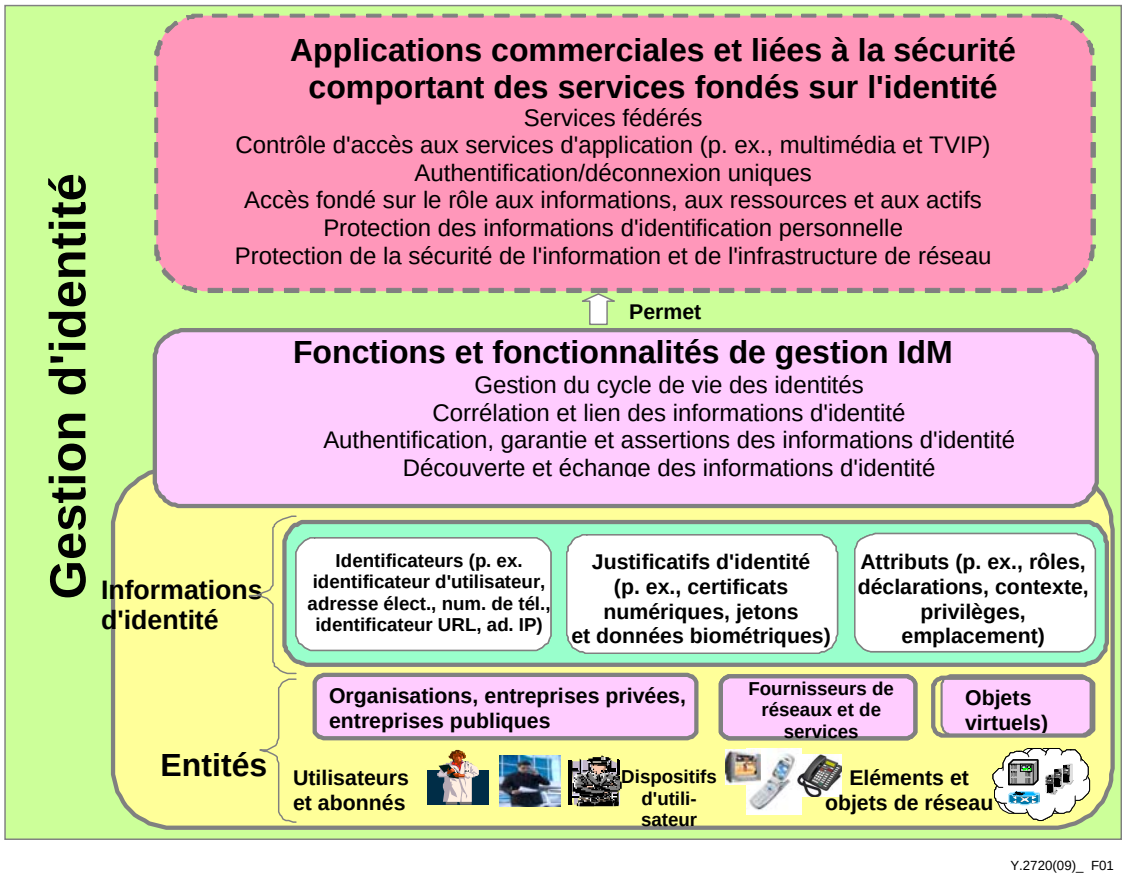


Figure 1 – Présentation de la gestion IdM

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

- identificateurs (par exemple, identificateurs d'utilisateur, adresses électroniques, numéros de téléphone, identificateurs uniformes de ressources et adresses IP);
- justificatifs d'identité (par exemple, certificats numériques, jetons et données biométriques); et
- attributs (par exemple, rôles, déclarations, privilèges, comportements et emplacement).

Les fonctions et fonctionnalités IdM sont utilisées pour garantir les informations d'identité et l'identité d'une entité, ainsi que pour prendre en charge des applications commerciales et liées à la sécurité, y compris des services fondés sur l'identité.

En outre, les services et fonctionnalités IdM permettent aux utilisateurs/entités abonnées de contrôler l'utilisation et la dissémination de leurs informations d'identité. La gestion IdM permet également aux membres d'une fédération (par exemple, des partenaires commerciaux) d'échanger et d'utiliser des informations d'identité fédérée afin de prendre en charge des services fédérés.

La gestion IdM permet la mise au point de différentes applications, notamment:

- *Des applications commerciales*
  - authentification et déconnexion uniques (par exemple, accès à plusieurs applications et services sans avoir à authentifier séparément chaque plate-forme d'application ou de service);
  - services fédérés (par exemple, accès à des services de différents fournisseurs de services ou de différents fournisseurs NGN).
- *Des services fondés sur l'identité*
  - services d'identificateur, de justificatif d'identité et d'attribut;
  - services relais d'identité (correspondance et compatibilité des informations d'identité dans un environnement hétérogène);
  - services d'informations de profil.
- *Des applications liées à la sécurité*
  - contrôle de l'accès pour les services de réseau et d'application (par exemple, téléphonie IP, TVIP et données);
  - contrôle de l'accès à des informations, ressources et actifs fondé sur le rôle;
  - gestion des autorisations et des privilèges;
  - services de protection de la sécurité (par exemple, caractéristiques de sécurité visant à protéger les ressources d'infrastructure de réseau ainsi que les informations d'identité et les actifs des utilisateurs/abonnés);
  - protection des informations d'identification personnelle (PII).

Dans un environnement fédéré et à plusieurs fournisseurs de services, les services et fonctionnalités IdM sont utilisés pour découvrir et communiquer des informations afin d'établir la confiance dans la ou les identités d'une entité au sein de différentes entités de réseau telles que les abonnés/déclarants, les parties utilisatrices (par exemple, utilisateurs, fournisseurs de services et fournisseurs de réseaux) et les fournisseurs de services d'identités (par exemple, fournisseurs de justificatifs d'identité et fournisseurs de vérificateurs) dans les domaines réseau et sécurité. Par exemple, un fournisseur d'identités choisi (comme un fournisseur d'authentifications/de vérificateurs) peut vérifier les identificateurs, les justificatifs d'identité et les attributs associés à une identité et les communiquer, au moyen d'assertions, à une partie utilisatrice (par exemple, un fournisseur de services) afin de faciliter le contrôle d'accès, la prise de décisions commerciales et l'application des politiques en vigueur (par exemple, respect de la vie privée et protection des informations d'identification personnelle).

5.2 Avantages et utilité dans les applications

En plus d'assurer la sécurité des réseaux NGN, la gestion IdM permet et facilite l'apparition d'applications et de services commerciaux de réseaux NGN nouveaux (par exemple, applications intégrées fixes et mobiles et applications web). En particulier, les services, les fonctionnalités et les fonctions IdM prennent en charge une large gamme d'applications et de services pour les utilisateurs finals/abonnés, les entreprises privées (par exemple, les réseaux, les fournisseurs de services, les entreprises) et les entreprises publiques, comme le montre la Figure 2.

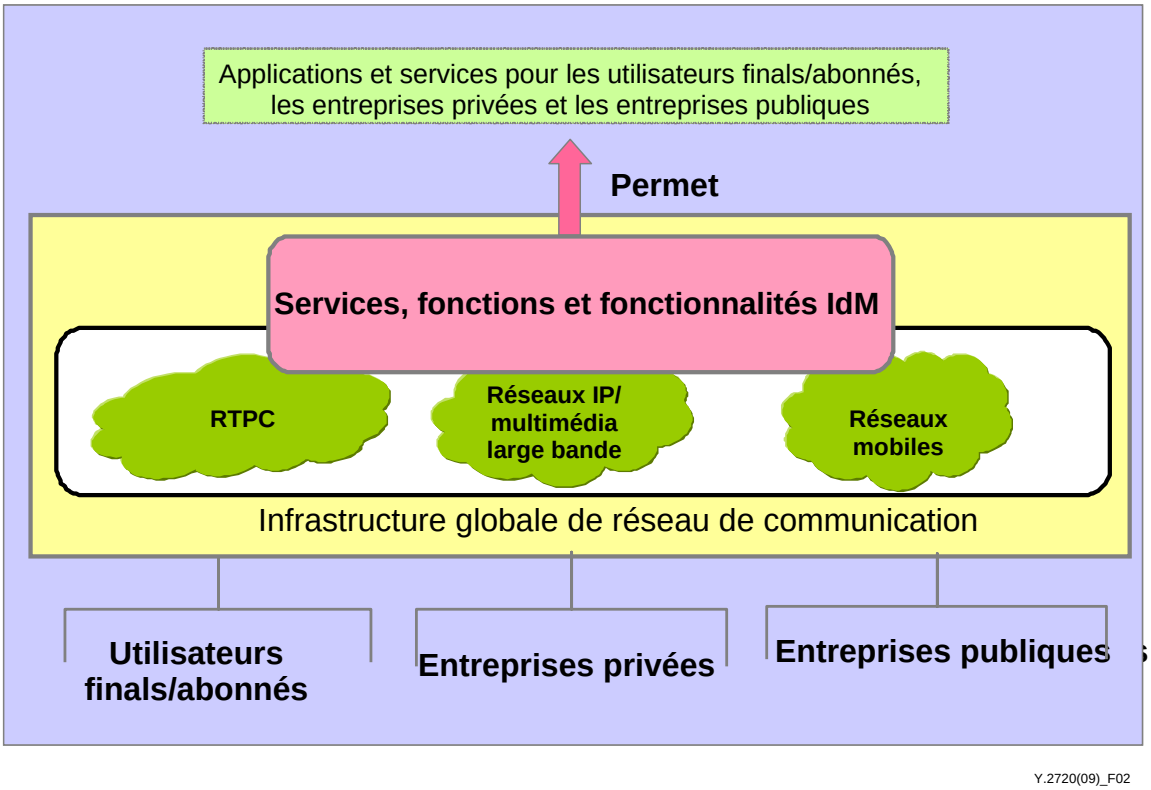


Figure 2 – Utilisation des services IdM

La gestion IdM est une composante essentielle de la gestion de la sécurité des réseaux NGN et de la prise en charge de l'accès nomade à la demande aux services et applications NGN souhaités par les utilisateurs finals à l'ère de l'information. Avec d'autres mécanismes de défense (par exemple les pare-feu, les systèmes de détection des intrusions et la protection contre les virus), elle joue un rôle important dans la protection de l'infrastructure NGN et des services et applications contre les cyberdélits tels que l'escroquerie et l'usurpation d'identité. En outre, puisque les utilisateurs seront sûrs que les transactions NGN seront sécurisées et fiables, la gestion IdM permettra de proposer de nouveaux services fondés sur l'identité. Elle permettra donc d'améliorer considérablement les services et les fonctionnalités de réseau existants. Le Tableau 1 récapitule les avantages et l'utilité de la gestion IdM.

Tableau 1 – Avantages et utilité de la gestion IdM

Point de vue	Avantages et utilité de la gestion IdM
Utilisateurs finals/abonnés	• Maîtrise par l'utilisateur des informations personnelles et protection des informations d'identification personnelle – Permettent de contrôler qui est autorisé à accéder (c'est-à-dire, de donner son consentement) aux informations personnelles et de quelle manière celles-ci sont utilisées. • Authentification et déconnexion uniques – Assurent un accès uniforme à plusieurs applications/services par l'intermédiaire de plusieurs fournisseurs de services/fédérations. • Contrôle d'accès souple pour les services de réseau et d'application (par exemple, téléphonie IP, TVIP et données). • Réseaux sociaux – Assurent des fonctionnalités d'identité dynamiques et souples pour accéder à des services de réseau social en toute confiance. • Sécurité – Assure la confiance dans les transactions avec une protection contre l'usurpation d'identité.
Entreprises privées (par exemple fournisseurs NGN)	• Permet d'accéder à des services d'abonnés n'importe où, n'importe quand et grâce à n'importe quel dispositif. • Permet des fonctions et des fonctionnalités de garantie de l'identité afin de prendre en charge plusieurs applications et services. • Assure une connexion dynamique/automatique entre plusieurs partenaires (par exemple, utilisateurs finals, réseaux visités et réseaux de rattachement) par rapport à des dispositions entre homologues visant à établir des accords de service, à échanger des informations d'identité et à appliquer une politique. • Permet de nouvelles applications et de nouveaux services (par exemple convergence fixe et mobile), y compris des services fondés sur l'identité tels que des services d'identificateurs, de justificatif d'identité et d'attributs, pour les abonnés et d'autres fournisseurs de services. • Prend en charge une interface API et un système de données normalisés afin de concevoir des applications pouvant être utilisées par des plates-formes de fourniture de services de plusieurs fabricants. • Permet une identité et des services fédérés. • Assure la protection des services d'application, de l'infrastructure de réseau et des ressources. • Simplifie le respect des dispositions réglementaires.
Entreprises publiques	• Permet des services et des fonctionnalités de garantie de l'identité et renforce le niveau de sécurité et de confiance dans les identités afin d'appuyer: – les services d'administration publique en ligne (par exemple, transactions web); – les services de sécurité du public (par exemple, services d'urgence de type 911); – les services d'application de la loi (par exemple, écoutes licites); – les services de télécommunications d'urgence; – les services d'alerte rapide; – les services de sécurité nationale. • Permet des services d'administration publique fédérés. • Assure la protection de l'infrastructure de communication (par exemple, contre les menaces à l'encontre de la cybersécurité).

5.3 Fournisseur d'identités (IdP)

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

Un fournisseur IdP est une entité qui crée, maintient et gère des informations d'identité sécurisées pour d'autres entités (par exemple, utilisateurs/abonnés, organisations et dispositifs) et propose des services fondés sur l'identité reposant sur une relation de confiance, commerciale ou d'une autre nature.

Dans un environnement à plusieurs fournisseurs de services, un fournisseur NGN peut être un fournisseur d'identités. Il peut en outre offrir des services IdP (par exemple, des services fondés sur l'identité) à d'autres fournisseurs. En outre, il est possible d'utiliser des services IdP de tiers.

5.4 Architecture fonctionnelle des réseaux NGN et utilisation des identificateurs

Comme indiqué dans [b-ITU-T Y.2012], *Prescriptions fonctionnelles et architecture du réseau de prochaine génération version 1*, un réseau NGN est composé de plusieurs éléments fonctionnels qui fonctionnent avec des identificateurs d'entités, l'objectif étant de prendre en charge et de faciliter des services et des applications. La Figure 3 montre des exemples d'identités qui peuvent être regroupées dans un diagramme fonctionnel des réseaux NGN correspondant à l'architecture NGN présentée dans [b-UIT-T Y.2012].

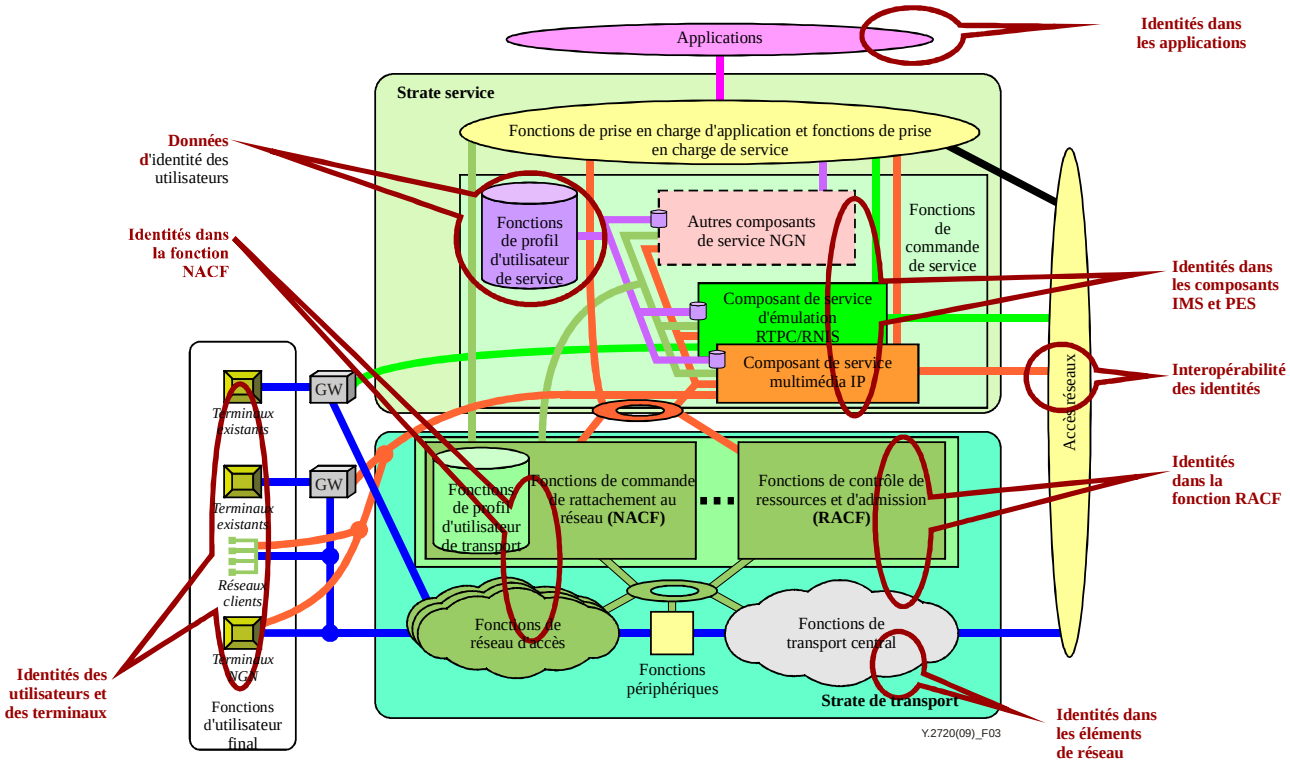


Figure 3 – Exemples d'identités dans un réseau NGN

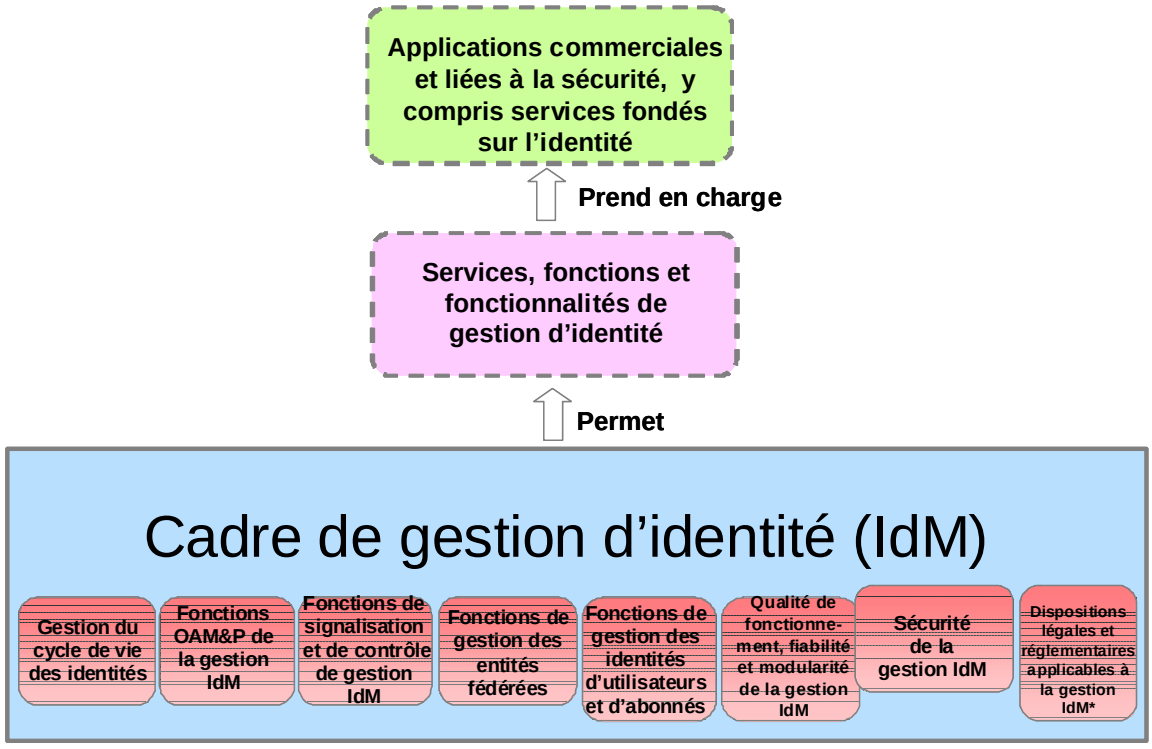
Puisque toutes les opérations NGN utilisent ces différentes identités, il est important de préserver leur intégrité. La gestion IdM comprend des services, des fonctionnalités et des fonctions de garantie permettant de préserver leur intégrité, dans le cadre de leur utilisation.

Dans un environnement de réseau NGN, une seule entité peut avoir plusieurs attributs d'identité. Ces attributs peuvent être utilisés par différents éléments de réseau (par exemple, dans différents domaines fournisseur NGN ou différentes strates du réseau NGN (par exemple, la strate service ou la strate transport)), et par différentes entités à différents emplacements. La gestion IdM doit donc

comprendre des fonctionnalités qui permettent l'échange sécurisé d'informations entre entités (et/ou emplacements) telles que les parties utilisatrices (par exemple, les fournisseurs d'applications ou de services) et les fournisseurs d'identités (IdP). Il est à noter que le fournisseur NGN peut également être un fournisseur IdP. L'échange d'informations IdM repose sur des politiques convenues et sur la confiance établie entre ces entités dans un environnement à plusieurs fournisseurs de services. Cette confiance dépend de l'assertion et de la validation des identités des entités dans les réseaux NGN répartis. La gestion IdM permet également de protéger la confidentialité des informations sur les entités (par exemple, attributs d'identité particuliers) et de garantir que seules les informations ayant fait l'objet d'une autorisation sont disséminées sur les réseaux NGN.

6 Présentation du cadre de gestion IdM

Ce cadre est organisé comme indiqué à la Figure 4.



*Note: Les dispositions légales et réglementaires ne relèvent pas du présent cadre, mais apparaissent dans cette figure par souci d'exhaustivité.

Figure 4 – Présentation du cadre de gestion IdM

Le cadre est composé des fonctions et des fonctionnalités IdM suivantes:

1) Gestion du cycle de vie des identités

   Il s'agit des processus et des fonctions de gestion du cycle de vie des identités et des informations d'identité (par exemple, les identificateurs, les justificatifs d'identité et les attributs). La gestion du cycle de vie des identités fait intervenir les processus et les procédures associés à la création et à l'émission d'une identité, de données et d'informations se rapportant à l'identité d'une entité.

2) Fonctions d'exploitation, d'administration, de maintenance et d'approvisionnement (OAM&P) de la gestion d'identité (IdM)

Il s'agit des fonctions et des fonctionnalités d'exploitation, d'administration, de maintenance et d'approvisionnement (OAM&P) spécifiquement liées à la prise en charge de la gestion IdM. La fonction OAM&P est un ensemble de fonctions de gestion qui assurent la détection d'erreurs, le contrôle de la qualité de fonctionnement, la gestion de la sécurité, des fonctions de diagnostic, la configuration et l'approvisionnement pour l'utilisateur pour un système ou un réseau. En particulier, elle comprend des fonctions et des fonctionnalités prises en charge par des systèmes de gestion réseau, généralement appelés système d'appui à l'exploitation (OSS, *operations support system*) et système d'appui aux activités (BSS, *business support system*).

3) Fonctions de signalisation et de contrôle de gestion d'identité (IdM)

Il s'agit des fonctions et des fonctionnalités de signalisation et de contrôle utilisées pour prendre en charge des services, des fonctionnalités et des fonctions IdM. Cela comprend la signalisation et le contrôle des communications en temps réel et en temps quasi réel.

4) Fonctions de gestion des identités fédérées

Il s'agit des fonctions et des fonctionnalités pour les fédérations d'identité et l'appui aux services fédérés.

5) Fonctions de gestion des identités d'utilisateurs et d'abonnés

Il s'agit des fonctions et des processus permettant aux utilisateurs finals et aux abonnés de contrôler les informations relatives à leur identité (par exemple, informations PII, préférences personnelles et emplacement). Cela comprend des fonctions permettant de contrôler, de déléguer et d'autoriser l'utilisation et la dissémination d'informations d'identité.

6) Qualité de fonctionnement, fiabilité et modularité de la gestion d'identité (IdM)

Il s'agit des fonctions et des procédures liées à la qualité de fonctionnement, à la fiabilité et à la modularité des systèmes et des solutions IdM.

7) Sécurité de la gestion d'identité (IdM)

Il s'agit des fonctions et des procédures liées à la protection de la sécurité des systèmes, services et fonctionnalités IdM.

8) Dispositions légales et réglementaires applicables à la gestion d'identité (IdM)

Les dispositions légales et réglementaires ne relèvent pas de la présente Recommandation.
NOTE – Cet élément n'est donné que par souci d'exhaustivité.

La section 8 contient une description détaillée de chaque élément.

7 Gestion IdM dans le contexte des architectures et des modèles de référence pour les réseaux NGN

7.1 Relations générales avec les architectures et services NGN

La Figure 5 illustre la relation du cadre de gestion IdM dans le contexte élargi de réseaux NGN.

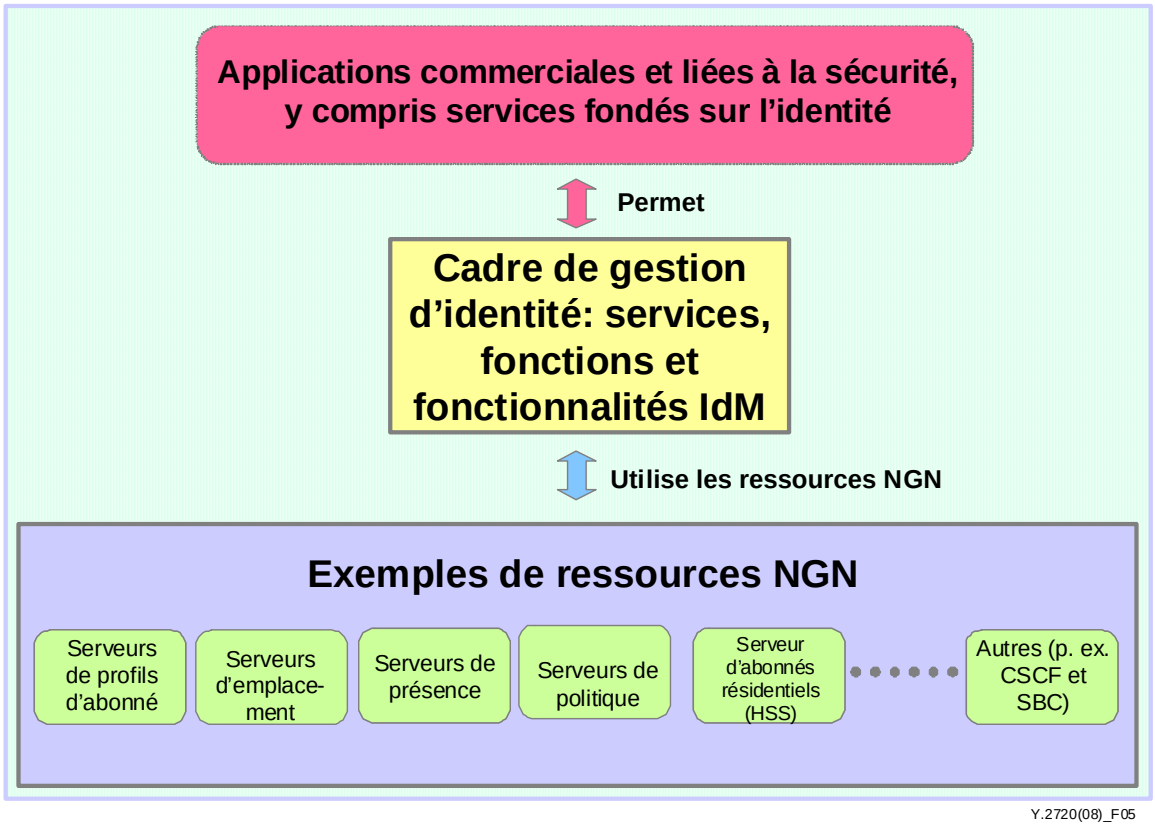


Figure 5 – Relation avec les architectures et services NGN

Comme le montre ce schéma, le cadre utilise les ressources du réseau NGN (par exemple, des informations stockées dans les serveurs d'abonnés, d'emplacement, de politique, de présence et d'abonnés résidentiels et dans d'autres éléments de réseau comme la fonction de commande de session d'appel (CSCF) et le contrôleur de session en limite (SBC)). Les services, les fonctions et les fonctionnalités IdM assurés par ce cadre servent à prendre en charge et à renforcer des applications commerciales et liées à la sécurité, y compris des services fondés sur l'identité.

7.2 Modèles de référence contenus dans la Recommandation UIT-T Y.2011 (Principes généraux et modèle de référence général pour les réseaux de prochaine génération)

La présente partie décrit les services, les fonctions et les fonctionnalités IdM dans le contexte des modèles et des références d'architecture pour les NGN définis dans [UIT-T Y.2011], *Principes généraux et modèle de référence général pour les réseaux de prochaine génération*.

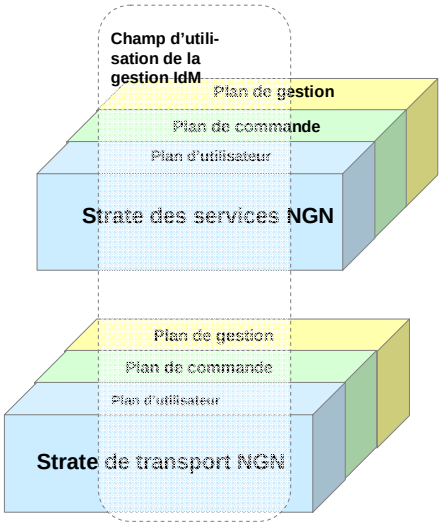


Figure 2/Y.2011

Figure 6 – Champ d'utilisation de la gestion IdM dans le contexte de la Figure 2 de [UIT-T Y.2011]

La Figure 6 montre le champ d'utilisation de la gestion IdM dans le cadre du modèle d'architecture de référence pour les NGN défini dans la Figure 2 de [UIT-T Y.2011]. Elle montre que l'on peut trouver des fonctions IdM dans les plans d'utilisateur, de commande et de gestion.

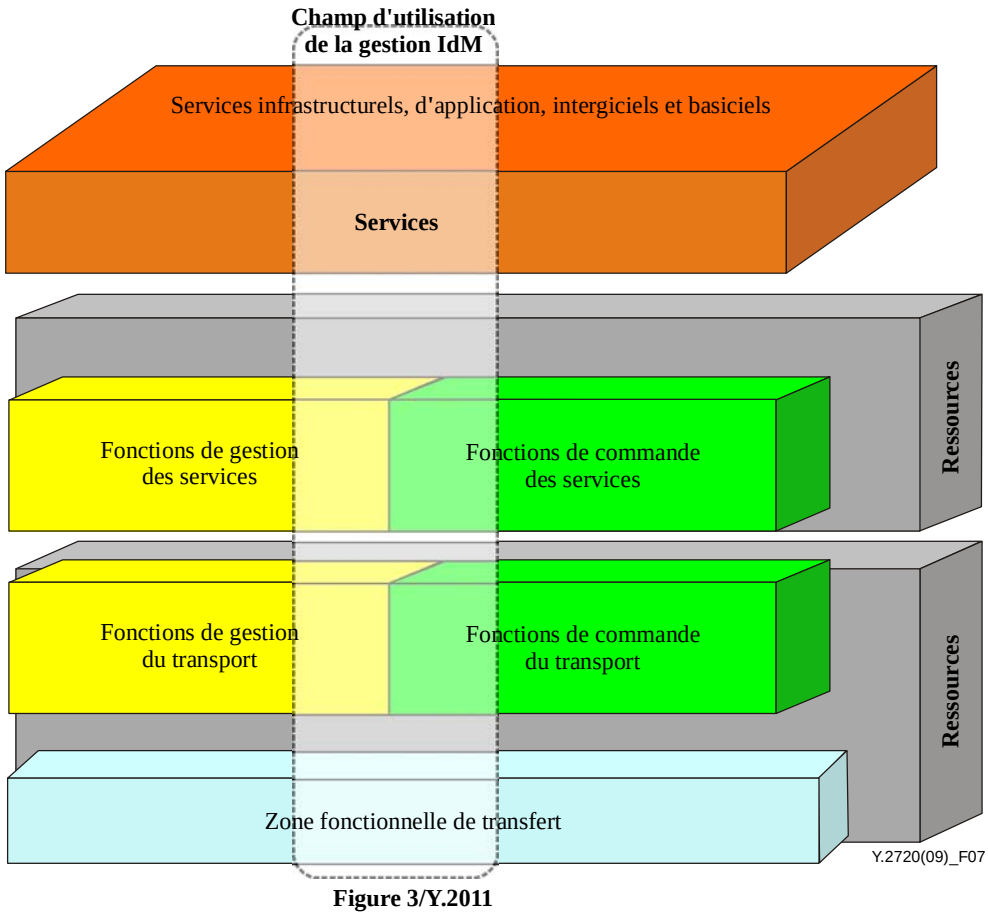


Figure 7 – Gestion IdM dans le cadre de la Figure 3 de [UIT-T Y.2011]

La Figure 7 montre le champ d'utilisation de la gestion IdM dans le cadre du modèle d'architecture de référence pour les NGN défini dans la Figure 3 de [UIT-T Y.2011]. Elle montre que l'on peut trouver des fonctions IdM dans toutes les couches verticales de l'architecture NGN.

8 Cadre de gestion d'identité

La présente section contient une description détaillée des groupes fonctionnels énumérés dans la section 6.

8.1 Gestion du cycle de vie des identités

8.1.1 Vérification et inscription

La création d'une identité pour une entité (par exemple, abonné, dispositif, organisation, fournisseur NGN ou objet) commence par le processus de vérification et d'inscription de l'identité ou du justificatif d'identité, c'est-à-dire par la souscription d'une identité ou d'un justificatif d'identité associé à une entité donnée qui peut reposer sur un contexte particulier (par exemple rôles).

Dans le cas d'utilisateurs finals, il s'agit du processus dans le cadre duquel un demandeur effectue des démarches pour s'abonner aux services d'un fournisseur IdP ou d'un fournisseur NGN.

Dans ce cas, le nom de l'abonné peut être un nom vérifié. Un nom vérifié est associé à l'identité d'une entité. Avant de recevoir un justificatif d'identité ou un jeton d'inscription pour le nom vérifié, le demandeur doit prouver que son identité est réelle et qu'il est bien l'entité habilitée à l'utiliser. Ce processus est appelé vérification d'identité. Une fois le nom vérifié, il peut être associé à des pseudonymes afin de permettre l'anonymat.

La vérification consiste à vérifier les attributs et les déclarations associés à une identité. Elle fait appel à des processus et à des procédures visant à vérifier et à valider une information lors de l'inscription d'une entité dans un système d'identités.

L'efficacité de la gestion IdM dans son ensemble dépend au départ des processus de vérification et d'inscription. Il est nécessaire de disposer de spécifications bien définies en matière de garantie et de mettre en place des procédures de politique et de gestion adaptées afin que le processus d'inscription dans son ensemble soit correctement conçu et mis en œuvre.

Il convient de prendre en considération les points suivants:

- Formation du personnel participant au processus d'inscription.
- Qualité des documents et des autres preuves appuyant l'inscription d'une entité.
- Processus permettant d'éviter les usurpations d'identité au moment de l'inscription.
- Processus permettant d'éviter plusieurs inscriptions pour une même entité.

8.1.2 Emission et révocation

Une fois le processus d'inscription effectué avec succès, un moyen (par exemple un justificatif d'identité) grâce auquel l'entité pourra être authentifiée dans l'avenir est fourni. Par exemple, un fournisseur IdP (ou un fournisseur NGN) émet un justificatif d'identité lié à l'identité ou à l'attribut (par exemple, privilège ou déclaration) se rapportant à l'identité d'une entité.

La révocation d'identité correspond à l'annulation d'une identité et des justificatifs associés. La partie ou le système (fournisseur IdP ou NGN) qui émet l'identité ou un justificatif est chargé de tenir à jour et de protéger les informations associées à l'identité. Il faut procéder à une révocation afin de ne pas continuer à utiliser une identité ou un justificatif qui n'est plus valable ou dont la sécurité n'est plus garantie.

Il convient de prendre en considération les points suivants:

- définition de critères d'émission et de révocation;
- définition de critères de mise à jour et de modification;
- synchronisation des informations d'identité;
- mise en place de processus et de procédures d'émission et de révocation;
- audit et examen des processus d'émission et de révocation;
- procédures et processus de notification d'émission, de mise à jour et de révocation d'identité ou de justificatif (en d'autres termes, tous les systèmes et processus intervenant dans la création d'une identité doivent pouvoir établir que l'identité ou les justificatifs en question ont été émis, actualisés et révoqués);
- procédures et processus bien définis concernant l'émission et la révocation d'une identité ou d'un justificatif et politique adaptée. Il est également nécessaire de disposer de procédures de gestion afin de veiller à la conception et à la mise en œuvre adéquates du processus dans son ensemble; et
- mécanismes de protection des processus et des procédures de révocation contre des menaces à l'encontre de la sécurité.

8.2 Fonctions OAM&P liées à la gestion d'identité

8.2.1 Modèle et schéma de données

Chaque fournisseur NGN, fédération ou entreprise peut utiliser des formats, des schémas qui lui sont propres, des définitions ou des sémantiques pour représenter et échanger des données et des informations d'identité. Par exemple, deux systèmes peuvent utiliser des représentations différentes pour une même information, comme la date de naissance (par exemple, mois/jour/année ou

jour/mois/année). De même, la sémantique, les schémas et les protocoles utilisés pour demander et échanger des informations d'identité peuvent être différents, ce qui peut donner lieu à des problèmes d'interopérabilité. Par exemple, dans le réseau téléphonique public commuté (RTPC), les informations d'identité comme le numéro ou l'identité de l'appelant, sont représentées avec une sémantique précise et extraites selon un protocole précis (par exemple, système SS7), et ne sont pas les mêmes que pour les systèmes de téléphonie IP utilisant le protocole SIP.

Il est important d'avoir recours à des solutions qui assurent l'interopérabilité entre systèmes IdM hétérogènes utilisant des modèles, des structures et des schémas de données différents.

Il convient de prendre en considération les points suivants:

- modèle et schémas de données permettant de faciliter l'interopérabilité entre systèmes IdM hétérogènes (par exemple, sources de données d'identité) dans le domaine d'un fournisseur NGN (c'est-à-dire, produits provenant de différents fournisseurs);
- modèle et schémas de données permettant de faciliter l'interopérabilité entre différents fournisseurs NGN (interréseau); et
- modèle et schémas de données permettant de faciliter l'interopérabilité entre différentes fédérations (par exemple, fournisseurs NGN et fournisseurs de services web).

8.2.2 Gestion de l'identificateur

La ou les identités d'une entité (par exemple, utilisateur/abonné, organisation, fédération, entreprise, fournisseur de services, dispositif et objet) qui doivent être gérées et tenues à jour peuvent être associées à un ou plusieurs identificateurs.

Un identificateur est une désignation utilisée pour représenter l'identité d'une entité, comme un identificateur d'utilisateur, un identificateur de réseau, une adresse électronique, un pseudonyme, un nom de groupe, etc. Les identificateurs suivants peuvent, par exemple, être associés à l'identité d'un utilisateur/abonné:

- identificateur d'utilisateur;
- adresse électronique;
- numéro de téléphone;
- identificateur uniforme de ressources;
- adresse IP.

L'efficacité de la gestion IdM dans son ensemble dépend de la garantie de pouvoir établir une corrélation et un lien entre les différents identificateurs afin de garantir l'identité d'une entité. Il faut donc disposer de spécifications et de procédures bien définies pour gérer les identificateurs.

Les points à prendre en considération pour la conception et la mise en œuvre de la gestion IdM sont les suivants:

- Différents types d'identificateurs avec diverses caractéristiques devront être gérés. Par exemple, certains identificateurs peuvent être globaux (c'est-à-dire le même dans différentes fédérations), prendre la forme de pseudonymes qui sont significatifs à l'intérieur d'un système ou être un identificateur "à usage unique" dont la validité est temporaire.
- Les identificateurs peuvent présenter différentes caractéristiques concernant la confidentialité afin que les décisions des utilisateurs ne puissent pas faire l'objet de recoupements abusifs.

8.2.3 Gestion des attributs

Les attributs d'identité sont des descripteurs d'une entité, par exemple, un type d'entité, une adresse IP préférée, un domaine, des informations d'adresse ou un numéro de téléphone. Les attributs peuvent aussi contenir des déclarations, des droits, des privilèges, des listes de délégués et

des restrictions spéciales. D'autres types d'attributs contiennent des informations suivies pour la détection des intrusions, comme les tentatives avortées d'assertion d'identité, les compteurs de renouvellement de clé, etc.

L'efficacité de la gestion IdM dépendrait de la garantie de pouvoir établir une corrélation et un lien entre les attributs afin de garantir l'identité d'une entité. Cela inclut le stockage et la fourniture d'attributs. Il faut donc mettre en place des spécifications et des procédures bien définies pour gérer les attributs.

Type particulier d'attribut, le profil est une caractéristique quelconque associée au comportement d'une entité. Les informations de profil peuvent être attribuées par des systèmes IdM compte tenu de la réputation et des interactions passées. Elles ne sont pas fixées par l'entité proprement dite. Pour évaluer la garantie de l'identité, on peut par exemple utiliser l'adresse IP, le point d'accès, les informations d'emplacement, la durée d'utilisation et les systèmes ayant fait l'objet d'un accès. Des fonctionnalités intelligentes peuvent en outre prendre en considération les événements actuels pour prédire les futurs profils d'utilisation.

Les points qu'il convient de prendre en compte pour la gestion des attributs sont les suivants:

- l'information de profil peut être considérée comme une information PII;
- spécifications et procédures strictes pour gérer les informations de profil;
- utilisation des informations de profil afin de minimiser le risque d'usurpation d'identité; et
- respect de la politique en matière d'informations PII.

8.2.4 Gestion des justificatifs d'identité

Les justificatifs d'identité sont utilisés afin d'authentifier une identité déclarée. Ils peuvent être:

- un nom d'utilisateur/mot de passe;
- un certificat numérique;
- un jeton et une carte intelligente;
- des indications de sécurité;
- des informations relatives à l'infrastructure de clé publique (PKI) comme des clés, des certificats, une autorité de signature des certificats, des informations cryptographiques, etc.; et
- des données biométriques.

La gestion des justificatifs d'identité d'une entité regroupe les activités opérationnelles qui visent à créer, émettre et gérer des informations utilisées pour authentifier les déclarations d'identité. L'efficacité de la gestion IdM dépend des processus, des procédures et des fonctionnalités de gestion des justificatifs d'identité. Il faut donc disposer de spécifications et de procédures bien définies pour gérer les justificatifs d'identité.

Les points qu'il convient de prendre en compte pour gérer les justificatifs d'identité sont les suivants:

- élaboration et tenue à jour de politiques dans le domaine des justificatifs d'identité;
- processus et procédures de gestion du cycle de vie des justificatifs (sous-ensemble de la gestion du cycle de vie des identités présentée au § 8.1); et
- politiques et accords de service dans des environnements à plusieurs fournisseurs de réseaux/services (négociations de politiques en matière de justificatifs d'identité, respect des besoins des fédérations, publication des informations relatives aux justificatifs d'identité telles que les clés publiques).

8.2.5 Journalisation et audit

Les fonctions et fonctionnalités de journalisation et d'audit jouent un rôle important dans l'efficacité des solutions IdM. Les mesures d'audit et de conformité incluent par exemple la tenue de journaux de sécurité pour pouvoir établir des responsabilités, la protection et l'utilisation appropriées des informations personnelles ainsi que la fourniture de notifications aux systèmes et entités appropriés (par exemple, propriétaires d'identité).

Les lignes directrices applicables à la journalisation et à l'audit sont les suivantes:

- journalisation et audit des événements liés à la gestion IdM (par exemple, accès à l'information d'identité, tentatives d'accès non autorisé, mises à jour des horodates, etc.) pour permettre une analyse judiciaire;
- mécanismes et procédures permettant de remonter à l'origine d'un problème;
- détection en cas de non-respect des politiques en vigueur; et
- respect des dispositions réglementaires nationales.

8.3 Fonctions de signalisation et de contrôle de la gestion d'identité

8.3.1 Introduction

Les fonctions de signalisation et de contrôle servent à découvrir et à communiquer des informations d'identité sécurisées (par exemple, identificateurs, attributs, déclarations) associées à une entité (par exemple, utilisateur/abonné, groupe, organisation, élément de réseau, fournisseur de services) afin de prendre en charge des services, fonctions et fonctionnalités IdM.

La présente section décrit les fonctions de signalisation et de contrôle associées à la gestion IdM.

8.3.2 Découverte de l'information d'identité

Dans un environnement réparti tel que les réseaux NGN, une information d'identité peut se trouver dans différents éléments de réseau (par exemple, serveur d'abonnés, serveur d'emplacement, serveur de présence, serveur d'abonnés résidentiels, etc.). Des moyens structurés permettant de découvrir des sources d'information d'identité font partie intégrante de la gestion IdM. Pour utiliser une information d'identité, une application doit savoir que ladite information existe. Dans un environnement NGN dynamique et évolutif, les informations d'identité et les sources d'informations d'identité doivent être elles aussi dynamiques. Par conséquent, les parties utilisatrices et les entités (par exemple, applications) auraient besoin de moyens structurés pour apprendre l'existence d'informations d'identité et les découvrir. Cela comprend également la découverte des fonctions, des services et des fonctionnalités de la fonction IdM.

Les points à prendre en considération pour spécifier et mettre en œuvre les fonctionnalités de découverte sont les suivants:

- découverte à l'intérieur du domaine d'un fournisseur NGN (intraréseau);
- découverte entre les domaines des différents fournisseurs NGN (interréseaux); et
- découverte entre membres de fédérations. Voir § 8.4.2 (Découverte de la fédération).

La découverte comprend également les fonctionnalités permettant de trouver ou de localiser les fournisseurs IdP. Elle est nécessaire dans le cadre de gestion IdM des réseaux NGN car ce cadre peut comprendre plusieurs fournisseurs IdP. Lorsqu'il n'y a qu'un seul fournisseur IdP (par exemple une entreprise), il n'est pas nécessaire de prévoir une fonction de découverte car on saura où obtenir les attributs d'identité. En outre, dans un réseau avec un seul fournisseur NGN, plusieurs systèmes peuvent assurer différentes fonctions liées à la gestion d'identité et des fonctions de découverte adaptées.

La découverte ressemble à une recherche d'identité web. On entre les caractéristiques d'identité dans le moteur de recherche et on obtient une liste d'identificateurs et de fournisseurs IdP qui

correspondent au besoin. Du fait de ce scénario avec des requêtes et des réponses, les fournisseurs IdP doivent en règle générale s'enregistrer eux-mêmes en tant que fournisseur d'un service d'identités particulier pour un utilisateur/dispositif donné.

Les méthodes que l'on peut utiliser pour prendre en charge les besoins associés à la découverte et à l'accès faisant autorité sont classées dans deux grandes catégories: 1) la découverte par comparaison d'origine, et/ou 2) la découverte par déduction. La première méthode prévoit qu'une entité assure la fonction de registre de référence des espaces nominatifs avec un serveur d'appui, tandis que la seconde méthode repose sur des règles bien connues grâce auxquelles l'adresse d'un serveur d'appui peut être obtenue de manière récurrente. Il est également possible de combiner ces deux méthodes.

8.3.3 Communications IdM

Il s'agit des fonctionnalités et des fonctions permettant de découvrir et d'échanger une information d'identité (par exemple, identificateurs, justificatifs d'identité et attributs) associée à l'identité d'une entité située dans des systèmes réseaux différents (par exemple, dans un serveur d'abonnés, d'emplacement, de présence, etc.) à l'intérieur du réseau d'un fournisseur NGN qui pourrait faire l'objet d'une corrélation et d'une vérification (à savoir par un serveur d'applications IdM assurant des fonctions d'authentification et de corrélation) afin de fournir des fonctionnalités de garantie d'identité. Les assertions d'identité et les attributs associés (par exemple, les déclarations et les privilèges) peuvent être communiquées aux systèmes utilisateurs (par exemple, services d'application) afin de prendre une décision concernant le contrôle d'accès. Les différents services d'application (par exemple, des plates-formes de fabricants différents) pourraient ainsi utiliser une infrastructure IdM commune au lieu de solutions indépendantes et autonomes. Les relations de communication à prendre en considération sont les suivantes:

- intraréseau: communications avec le domaine d'un fournisseur NGN (par exemple, entre éléments de réseau);
- interréseaux: communications entre deux fournisseurs NGN différents; et
- fédération: communications entre membres d'une fédération.

8.3.3.1 Communications en temps réel et en temps quasi réel

La solution utilisée pour découvrir et échanger une information d'identité doit être choisie selon qu'il est nécessaire d'avoir des communications en temps réel ou en temps quasi réel. Cela dépendra des applications particulières prises en charge.

8.3.3.2 Protocoles et interfaces de signalisation et de contrôle

La Figure 8 montre les interfaces externes qui peuvent être utilisées pour prendre en charge des communications IdM. Par exemple, certaines interfaces sont utilisées pour échanger des informations d'identité ou contrôler des services, des fonctions et des fonctionnalités IdM.

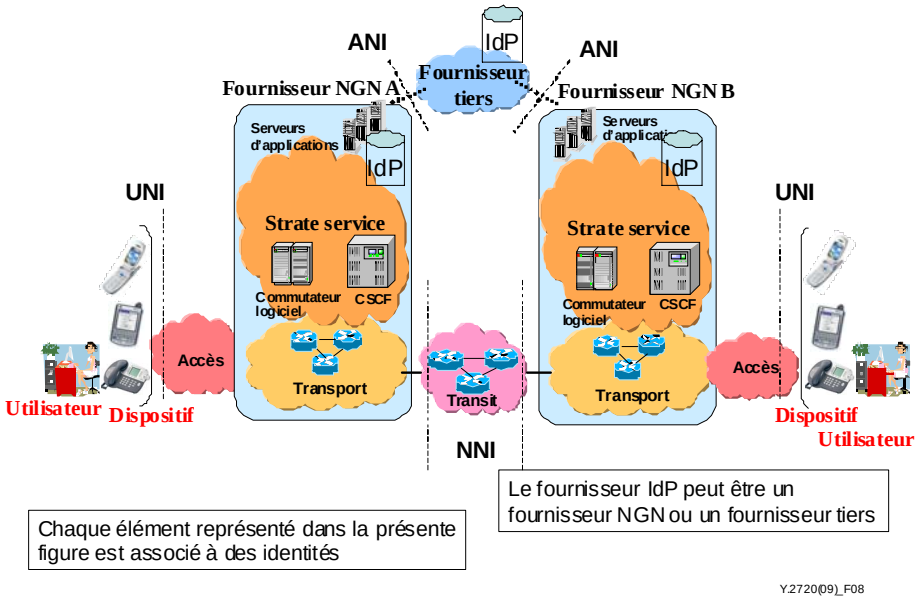


Figure 8 – Interfaces externes

Les interfaces externes sont:

- les interfaces utilisateur-réseau (UNI);
- les interfaces application-réseau (ANI); et
- les interfaces réseau-réseau (NNI).

Le choix des spécifications et des protocoles spécifiques à utiliser dépend de l'interface, de l'information à communiquer ou des fonctions de contrôle à réaliser. Il conviendrait d'identifier et de définir des spécifications particulières, des protocoles possibles et des profils à utiliser afin de faciliter l'interopérabilité. Les solutions d'interface dépendent de facteurs tels que les besoins particuliers des applications et des services (par exemple, temps réel ou temps quasi réel), des protocoles (par exemple, SAML, Diameter, RADIUS) ainsi que des mécanismes et des méthodes (par exemple, [b-UIT-T X.509] et architecture d'amorçage générique (GPA)).

Outre les interfaces externes, les interfaces internes sont également importantes dans le choix de solutions d'ensemble. Dans un réseau NGN, une information d'identité peut se trouver dans différents éléments ou services d'application (par exemple, serveur d'abonnés, d'emplacement et de présence ou dans d'autres éléments de réseau comme la fonction CSCF et le contrôleur SBC). Il est important de tenir compte des interfaces internes et des protocoles à utiliser pour découvrir et échanger des informations d'identité si l'on veut assurer l'interopérabilité entre les produits de plusieurs fabricants.

8.3.3.3 Mécanismes et procédures

Il conviendrait d'identifier et de spécifier les mécanismes et les procédures utilisées pour mettre en œuvre une fonction ou une fonctionnalité IdM donnée. Il faudrait identifier et spécifier des mécanismes ou protocoles précis ainsi que l'endroit et le mode d'utilisation. Ces mécanismes et protocoles peuvent par exemple être:

- SAML;
- X.509;

- GBA; et
- E.115.

8.3.4 Corrélation et lien

Les informations d'identité (par exemple, les identificateurs, les justificatifs d'identité et les attributs) peuvent faire l'objet d'une corrélation afin d'établir un lien pour garantir l'identité d'une entité. Ainsi, l'information d'identité associée à un abonné (par exemple, l'identificateur d'utilisateur), ou à un dispositif d'abonné (par exemple, l'identificateur de dispositif) et l'information d'emplacement peuvent faire l'objet d'une corrélation afin d'établir un lien qui offre une meilleure garantie concernant l'abonné.

Les points dont il faut tenir compte lorsqu'on spécifie et met en œuvre la corrélation et le lien sont les suivants:

- application de la politique en vigueur (par exemple, politique en matière d'anonymat ou de confidentialité).

8.3.5 Authentification

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

En règle générale, on établit la confiance en attribuant un identificateur d'utilisateur et un mot de passe pour chaque système. Toutefois, dans le cadre des réseaux NGN, cette approche n'est pas souhaitable, n'est pas efficace du point de vue du fonctionnement et peut entraîner des pratiques non sécurisées. Les points à prendre en considération lorsqu'on spécifie et met en œuvre l'authentification sont:

- la confidentialité et l'intégrité des mécanismes d'authentification;
- des justificatifs d'identité suffisamment sûrs pour recevoir la confiance des systèmes.

8.3.6 Garantie d'authentification

La garantie d'authentification est le processus permettant d'établir la confiance dans les identités et les déclarations qui sont présentées à un système informatique. Toutes les informations utilisées pour l'authentification ne devraient pas être traitées de la même manière, ni avoir nécessairement la même valeur de garantie. Par exemple, la confiance que l'on peut accorder à une authentification par données biométriques est très différente de celle que l'on peut accorder à une authentification par identificateur d'utilisateur et mot de passe. Il convient d'attribuer à chaque identificateur une valeur relative sur la base des principes fondamentaux afin de quantifier la confiance dans le fait qu'une entité authentifiée est bien la bonne entité.

L'objectif de la garantie d'authentification est de quantifier les chances qu'une entité soit bien celle ou ce qu'elle prétend être. Tous les identificateurs utilisés dans un processus de décision d'authentification ne sont pas traités de la même manière et n'ont pas nécessairement la même valeur. En outre, plus les conséquences d'une erreur d'authentification sont graves, plus le niveau requis de garantie d'authentification devrait être élevé, en fonction des risques encourus (par exemple, incidence critique).

Un mécanisme permettant de quantifier et de communiquer la garantie d'authentification permet aux parties utilisatrices de prendre des décisions relatives à la confiance qu'elles peuvent accorder au processus d'authentification utilisé pour valider l'identité ou les déclarations d'une entité.

L'un des principaux avantages de la garantie d'authentification est la possibilité de déterminer le niveau de confiance dans le fait qu'une entité est bien ce qu'elle prétend tout au long du cycle de vie de l'identité. Pour prendre en charge des services fédérés et assurer la protection de la cybersécurité, il est essentiel de disposer de critères normalisés pour attribuer et communiquer des valeurs relatives de garantie pour le processus, les mécanismes et les données d'authentification (par exemple, mot de passe, justificatifs d'identité, données biométriques).

Un processus de garantie d'authentification devrait tenir compte des points suivants:

- Mécanisme d'authentification: des mots de passe permanents sont plus faibles que des mots de passe dont la durée de validité est limitée, et un jeton matériel avec un numéro d'identification personnel est en règle générale plus efficace qu'un jeton logiciel.
- Protocole d'authentification: en règle générale, on considère qu'un protocole qui est réputé sûr face aux attaques de l'intercepteur ou qui est fondé sur un fonctionnement cryptographique est solide.
- Caractéristiques du dispositif utilisé pour l'authentification: la confiance accordée à l'authentification repose en partie sur les caractéristiques du dispositif de l'utilisateur. En d'autres termes, un ordinateur standard du commerce que l'organisation possède et contrôle ou un dispositif inviolable dédié est plus sûr qu'un dispositif standard du commerce accessible à tous.
- Emplacement de l'entité soumise à l'authentification: il conviendrait de tenir compte de l'emplacement de l'utilisateur (dans les locaux de l'entreprise, dans un kiosque public, dans un café Internet, etc.). La confiance sera plus grande s'il est difficile pour un terminal public situé dans un kiosque de convaincre le serveur d'authentification qu'il est situé à l'intérieur des locaux de l'entreprise.
- Voie de communication: en règle générale, l'authentification fait appel à une voie de communication (réseaux sans fil, lignes louées d'entreprise, etc.) entre l'entité soumise à l'authentification et le serveur assurant l'authentification et/ou prenant les décisions d'accès. L'information utilisée pour l'authentification doit être transmise de manière fiable au serveur d'authentification et ne doit pas pouvoir être piratée par un intrus.
- Niveau de facilité avec laquelle il est possible de manipuler l'authentification par un comportement malveillant: il est important d'évaluer le risque associé à la compromission des clés cryptographiques.

8.3.7 Délégation

La délégation correspond aux actions et aux processus nécessaires pour transférer des privilèges d'une entité lui permettant de réaliser certaines actions pour le compte d'une entité principale vers une autre entité qui ne détient pas ces privilèges.

Par exemple, l'autorité de délégation commence avec la possibilité de définir quels comptes peuvent réaliser certaines actions de gestion (par exemple, la création de nouveaux comptes) ou gérer des fonctions particulières (par exemple, la modification du mot de passe pour un compte). Ainsi, étant donné qu'il est possible de déléguer les actions ou les activités d'administration, l'objectif est de fournir un environnement dans lequel cette tâche sera réalisée de manière sécurisée et responsable.

8.3.8 Application des politiques

Il devrait être tenu compte des politiques en vigueur dans la conception et la mise en œuvre de solutions IdM. Les mesures visant à assurer le respect de ces politiques concernent généralement les points suivants:

- anonymat et confidentialité;
- création et collecte d'informations d'identité; et
- utilisation et dissémination d'informations d'identité.

8.3.9 Prise en charge des services nécessitant un traitement prioritaire

La conception et la mise en œuvre de solutions IdM devraient tenir compte de la prise en charge des services d'application et des sessions de communication nécessitant un traitement prioritaire, comme un service de télécommunications d'urgence (ETS, *emergency telecommunication service*). Par exemple, toute interaction avec des systèmes IdM visant à établir et maintenir une session de communication pour des services de télécommunications d'urgence devrait être traitée en priorité. Voir [b-UIT-T E.107] et [b-UIT-T Y.2205] pour plus d'informations sur les services et les fonctionnalités nécessitant un traitement prioritaire.

8.4 Fonctions de gestion des identités fédérées

8.4.1 Identités fédérées

L'idée générale de la fédération est de permettre à chaque membre d'une fédération de rester indépendant tout en facilitant l'échange d'informations d'identité particulières à des fins de services fédérés. Par exemple, certaines informations sur l'identité d'un utilisateur/abonné (par exemple sous-ensemble de profil d'abonné) pourraient être fédérées (c'est-à-dire mises à la disposition des membres de la fédération).

8.4.2 Découverte de la fédération

La découverte d'une fédération correspond aux fonctions et aux mécanismes permettant de découvrir et d'échanger des informations sur une identité fédérée. Par exemple, certaines informations sur l'identité d'un utilisateur/abonné (telles qu'un sous-ensemble d'informations de profil d'abonné) peuvent être fédérées.

La découverte de fédération vise principalement à identifier ou à découvrir un fournisseur IdP candidat ou le fournisseur IdP qui est la source faisant autorité pour une information d'identité particulière associée à une entité (par exemple, information d'emplacement).

La découverte est nécessaire dans toute architecture à plusieurs fournisseurs IdP ou dans laquelle l'emplacement des fournisseurs IdP peut changer. Lorsqu'il n'y a qu'un seul fournisseur IdP (par exemple une entreprise), il n'est pas nécessaire d'avoir une fonction de découverte car la partie utilisatrice ou le fournisseur de services saura implicitement où obtenir les informations sur l'identité de l'entité.

8.4.3 Relais et interfonctionnement

En général, chaque fournisseur NGN, entreprise ou membre d'une fédération peut avoir des formats, des schémas, des définitions ou des sémantiques qui lui sont propres pour représenter et échanger des données et des informations d'identité. Par exemple, deux systèmes différents peuvent utiliser des représentations différentes pour une même information, comme la date de naissance. De même, la sémantique, les schémas et les mécanismes utilisés pour demander et échanger des informations d'identité peuvent être différents, ce qui peut donner lieu à des problèmes d'interopérabilité. Il faudra donc prévoir des fonctionnalités adaptées afin de permettre le relais et l'interfonctionnement.

8.5 Fonctions de gestion d'identité des utilisateurs et des abonnés

Il faut disposer de fonctions permettant à un utilisateur final/abonné de fournir des informations concernant le contrôle des informations d'identité qui les concernent pour que les solutions IdM soient efficaces. Cela comprend des fonctions et des fonctionnalités permettant à une entité, comme un utilisateur final/abonné, de communiquer aux fournisseurs de services et aux fournisseurs IdP des informations concernant les conditions, les restrictions, les consentements, les autorisations en matière de création, de collecte, d'utilisation et de dissémination de leurs informations d'identité.

Ces fonctions sont liées à l'application des politiques en vigueur, par exemple en matière de protection des informations PII et d'informations d'identité anonyme ou pseudonyme.

Les points à prendre en considération sont les suivants:

- moyens permettant aux utilisateurs finals/abonnés de transmettre une information à un fournisseur NGN concernant le contrôle de leurs informations d'identité;
- respect des politiques applicables en matière de protection des informations PII; et
- facilité d'utilisation pour l'utilisateur final/abonné.

8.6 Qualité de fonctionnement et fiabilité

8.6.1 Qualité de fonctionnement

Les fonctionnalités et les fonctions IdM seront utilisées pour prendre en charge et renforcer une large gamme d'applications commerciales et liées à la sécurité. Par exemple, les fonctions IdM peuvent servir à garantir l'identité d'entités de communication avant d'autoriser une session de communication (par exemple, session de téléphonie IP, de TVIP ou de données). Par conséquent, l'incidence de la gestion IdM en termes de qualité de fonctionnement sur les services d'application de niveau supérieur pris en charge (par exemple téléphonie IP, TVIP ou données) est importante pour l'efficacité de la solution dans son ensemble. Par exemple, la gestion IdM ne devrait pas avoir un effet négatif sur les services d'application de niveau supérieur pris en charge, et par voie de conséquence, nuire à la qualité de service (QoS) et à la qualité d'expérience (QoE) globales pour les utilisateurs finals/abonnés.

Il est important de tenir compte des aspects liés à la gestion de la qualité de fonctionnement lorsque l'on élabore des solutions IdM. La gestion de la qualité de fonctionnement comprend la collecte et l'analyse de données statistiques afin d'évaluer la qualité de fonctionnement. L'évaluation de la qualité de fonctionnement est l'évaluation systématique de la capacité d'un système réseau à s'acquitter de sa fonction grâce à la collecte et l'analyse en continu de données significatives concernant la qualité de fonctionnement. Les procédures d'évaluation de la qualité de fonctionnement visent à rendre compte d'erreurs et de problèmes intermittents dus à la détérioration progressive de l'équipement de réseau. Des techniques de maintenance préventives telles que l'évaluation de la qualité de fonctionnement permettent de détecter les problèmes avant qu'ils ne prennent de l'ampleur.

8.6.2 Précision des horodates

La précision des horodates est un facteur important pour la gestion IdM. L'audit décrit les événements qui se produisent pendant ces intervalles de temps. Dans le cadre de l'audit, les horodates sont essentielles et la qualité, voire l'utilisabilité, des données d'audit dépend de la précision des horodates.

La précision des horodates est déterminée par trois facteurs – la précision de lecture de l'horodate sur l'horloge locale, le calage de l'horloge locale sur une horloge de référence et l'incertitude mathématique de mesure relative à l'horloge locale par rapport à une référence.

8.6.3 Fiabilité et disponibilité

La fiabilité et la résilience des éléments et des systèmes réseaux assurant les fonctions et les fonctionnalités IdM constituent un aspect important de la conception et de la mise en œuvre de solutions car la gestion IdM servira à prendre en charge et à renforcer une large gamme d'applications commerciales et liées à la sécurité ayant peut-être des spécifications particulières en termes de disponibilité. Il faudra donc tenir compte de spécifications et de lignes directrices comme celles indiquées ci-après en ce qui concerne les facteurs de fiabilité:

- conceptions de systèmes (par exemple, redondance) concernant la solidité et la résilience; et
- diversité (par exemple, diversité géographique) concernant la disponibilité.

En outre, la conception et la mise en œuvre de solutions IdM devraient également prévoir des mesures en cas de défaillance. Par exemple, l'application utilisatrice pourrait autoriser certains privilèges limités si le système IdM dans son ensemble était défectueux ou indisponible.

8.7 Sécurité IdM

8.7.1 Protection de la sécurité des éléments de réseau assurant la gestion IdM

Etant donné que les informations et les ressources d'identité sont précieuses et sensibles et qu'elles servent à prendre en charge des applications et des services commerciaux, des éléments de réseau permettant des services, des fonctions et des fonctionnalités IdM seront la cible d'attaques contre la sécurité et devront par conséquent être protégés.

Des spécifications et des mesures adaptées afin de sécuriser et de protéger les éléments et les systèmes de réseaux assurant des fonctions, des services et des fonctionnalités IdM sont nécessaires. Il faut par exemple tenir compte des aspects liés à la sécurité mentionnés ci-dessous:

- protection de la sécurité des services, des fonctions et des fonctionnalités IdM;
- protection de la sécurité des interfaces de signalisation et de communication; et
- protection de la sécurité des interfaces de gestion des systèmes IdM (c'est-à-dire des interfaces utilisées pour configurer et gérer les informations d'identité).

8.7.2 Protection des informations d'identification personnelle (PII)

La protection des informations PII est un aspect extrêmement important de la gestion IdM. Il conviendrait de définir et mettre en œuvre des fonctionnalités spécifiques pour protéger ces informations. Ce point est lié à l'application des politiques en vigueur en matière de protection des informations PII, sous réserve des réglementations nationales et régionales. Il convient de tenir compte des fonctions et des fonctionnalités suivantes:

- fonctionnalités permettant aux utilisateurs/abonnés de communiquer des préférences en matière d'informations PII;
- fonctionnalités permettant d'assurer la transparence (c'est-à-dire fonctionnalités garantissant que seules les entités autorisées ont accès aux informations PII ou peuvent les consulter); et
- fonctionnalités permettant de fournir des notifications concernant la dissémination et l'utilisation des informations d'identité.

Bibliographie

[b-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.*

[b-UIT-T E.115] Recommandation UIT-T E.115 (2008), *Assistance informatisée à l'annuaire*.

[b-UIT-T X.509] Recommandation UIT-T X.509 (2005) | ISO/CEI 9594-8:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

[b-UIT-T X.810] Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général*.

[b-UIT-T X.811] Recommandation UIT-T X.811 (1995) | ISO/CEI 1081-2:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'authentification.*

[b-UIT-T X.911] Recommandation UIT-T X.911 (2005) | ISO/CEI 15414:2006, *Technologies de l'information – Traitement réparti ouvert – Modèle de référence – Langage d'entreprise*.

[b-UIT-T X.1121] Recommandation UIT-T X.1121 (2004), *Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout*.

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

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

[b-UIT-T Y.2012] Recommandation UIT-T Y.2012 (2006), *Prescriptions fonctionnelles et architecture du réseau de prochaine génération version 1*.

[b-UIT-T Y.2091] Recommandation UIT-T Y.2091 (2008), *Termes et définitions pour les réseaux de prochaine génération*.

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

[b-UIT-T Y.2701] Recommandation UIT-T Y.2701 (2007), *Prescriptions de sécurité des réseaux de prochaine génération de version 1*.

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

[b-ETSI EG 202 072] ETSI EG 202 072, V1.1.1 (2002), *Universal Communications identifier (UCI); Placing UCI in context; Review and analysis of existing identification schemes*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=14108>

[b-ETSI EG 202 236] ETSI EG 202 236, V1.1.1 (2003), *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Design guide; Use of non-numeric names*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=17732>

[b-ETSI EG 284 004] ETSI EG 284 004, V1.1.2 (2007), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Incorporating Universal Communications Identifier (UCI) support into the specification of Next Generation Networks*. <http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=21139>

[b-ETSI TS 102 042] ETSI TS 102 042, V1.3.4 (2007), *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*. <http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=27736>

[b-RFC 3650] IETF RFC 3650 (2003), *Handle System Overview*. <http://www.ietf.org/rfc/rfc3650.txt?number=3650>

[b-NIST] NIST SP800-63, v6.3.3, *Electronic Authentication Guidelines*. <http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>

[b-OGIM] The Open Group, *Identity Management White Paper* (03/2004). <http://www.opengroup.org/bookstore/catalog/w041.htm>

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, 2009