Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1251

(09/2009)

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

Sécurité du cyberespace – Gestion des identités

Cadre régissant le contrôle par l'utilisateur des identités numériques

Recommandation UIT-T X.1251

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

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

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

Recommandation UIT-T X.1251

Cadre régissant le contrôle par l'utilisateur des identités numériques

Résumé

La Recommandation UIT-T X.1251 définit un cadre permettant d'améliorer le contrôle et l'échange, par les utilisateurs, des informations relatives à leurs identités numériques. Elle définit également les capacités fonctionnelles et d'utilisateur concernant l'échange d'informations d'identité numérique. Les travaux consistent notamment à permettre à l'utilisateur de contrôler la diffusion d'informations personnellement identifiables.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1251	2009-09-25	17

Mots clés

Client d'identité numérique, contrat numérique, échange d'identité, gestion d'identité, identité, identité numérique, serveur d'identité.

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

TABLE DES MATIÈRES

Recommandation UIT-T X.1251[1]

Cadre régissant le contrôle par l'utilisateur des identités numériques

1 Domaine d'application

La présente Recommandation définit un cadre permettant d'améliorer le contrôle et l'échange par les utilisateurs des informations relatives à leurs identités numériques.

Elle définit également les capacités nécessaires pour l'échange d'informations d'identité numérique. Les travaux consistent notamment à permettre à l'utilisateur de contrôler la diffusion d'informations personnellement identifiables.

NOTE – Dans la présente Recommandation, l'emploi du terme "identité" relatif à la gestion d'identité (IdM) ne correspond pas à sa signification absolue et ne constitue pas en particulier une 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. Le Bureau de la normalisation des télécommunications de l'UIT tient la liste des Recommandations UIT-T en vigueur. 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 X.1205] Recommandation UIT-T X.1205 (2008), *Présentation générale de la cybersécurité*.

[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*.

3 Termes et définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes ci-après définis ailleurs:

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

3.1.2 entité [b-UIT-T X.1252]: tout 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 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.

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

---

[1] La présente Recommandation peut ne pas être applicable dans certains pays en raison de la législation nationale.

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

3.1.5 identité [b-UIT-T X.1252]: représentation d'une entité sous la forme d'un ou de plusieurs éléments d'information qui sont suffisants pour pouvoir distinguer les entités dans un contexte. Aux fins de l'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 (les attributs). Toutefois, l'identité holistique est théorique et échappe à toute description et utilisation pratique, car le nombre de tous les attributs possibles est indéfini.

3.1.6 gestion d'identité [b-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 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 réseau et de services, les éléments et objets de réseau et les objets virtuels); et
- permettre des applications commerciales et liées à la sécurité.

3.1.7 fournisseur de service d'identité (IdSP, *identity service provider*) [b-UIT-T X.1252]: entité qui vérifie, tient à jour, gère et peut créer et attribuer des informations d'identité d'autres entités.

3.1.8 informations personnellement identifiables (PII, *personally identifiable information*) [b-UIT-T Y.2720]: informations relatives à une quelconque personne vivante, permettant d'identifier l'individu en question (y compris les informations permettant d'identifier une personne lorsqu'elles sont combinées avec d'autres informations même si ces dernières n'identifient pas clairement la personne).

3.1.9 partie utilisatrice [b-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.

3.1.10 utilisateur [b-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.

3.1.11 centré sur l'utilisateur [b-UIT-T X.1252]: système IdM qui peut conférer à l'utilisateur (IdM) la capacité de contrôler et d'appliquer diverses politiques de respect de la vie privée et de sécurité régissant l'échange d'informations d'identité, en particulier des informations PII, entre entités.

3.2 Termes définis dans la présente Recommandation

Les termes suivants sont définis dans la présente Recommandation:

3.2.1 cercle de confiance: ensemble de critères établis pour regrouper des organisations au sein d'une fédération, afin de fournir un accès sécurisé aux ressources de chacune d'elles. Il est à noter qu'un cercle de confiance est également le résultat final du regroupement d'organisations au sein d'une fédération.

3.2.2 contrat numérique: contrat établi sous forme numérique et signé par deux entités entre lesquelles un accord a été conclu.

3.2.3 identité numérique: représentation numérique des informations connues à propos d'un individu, d'un groupe ou d'une organisation spécifique.

3.2.4 client d'identité numérique: programme client qui offre à l'utilisateur un service d'authentification et de gestion de justificatif d'identité, d'échange d'identité et de protection de la confidentialité.

3.2.5 fraude d'identité: délit qui consiste pour un imposteur à obtenir des éléments essentiels d'informations personnellement identifiables (PII) – numéros de sécurité sociale et numéros de permis de conduire par exemple – et à les utiliser à des fins d'enrichissement personnel.

3.2.6 informations d'identité: informations identifiant un utilisateur, y compris les adresses fiables (générées par le réseau) et/ou non fiables (générées par l'utilisateur).

3.2.7 échange d'identité: diffusion des informations d'identité d'un utilisateur entre un fournisseur de service d'identité et une partie utilisatrice par le biais d'un client d'identité numérique.

3.2.8 sélecteur d'identité: composant logiciel d'un client d'identité numérique mis à la disposition de l'utilisateur, par l'intermédiaire duquel l'utilisateur contrôle et communique ses identités numériques.

3.2.9 serveur d'identité: serveur qui gère les informations d'identité et de justificatif d'identité de l'utilisateur et les remet à un client d'identité numérique.

3.2.10 synchronisation d'identité: mise à jour des informations d'identité d'un utilisateur diffusées à une partie utilisatrice lorsque la source des informations d'identité dans un fournisseur de service d'identité est modifiée.

3.2.11 terminaison d'identité: suppression des informations d'identité d'un utilisateur stockées en mémoire lorsque leur validité a expiré.

3.2.12 jeton d'identité: modèle de données de l'identité numérique, qui peut contenir les informations PII et les informations de justificatif d'identité d'un utilisateur.

3.2.13 hameçonnage: activité frauduleuse qui consiste pour un individu à essayer d'obtenir des informations sensibles – nom d'utilisateur, mot de passe et numéro de carte de crédit, par exemple – en se faisant passer pour une entité digne de confiance dans une communication électronique.

3.2.14 politique de confidentialité: politique définissant les règles destinées à protéger l'accès aux informations confidentielles personnelles et leur diffusion.

4 Abréviations et acronymes

Les abréviations suivantes sont utilisées dans la présente Recommandation:

CoT cercle de confiance (*circle of trust*)

DIC client d'identité numérique (*digital identity client*)

DIIF cadre d'échange d'identité numérique (*digital identity interchange framework*)

IdM gestion d'identité (*identity management*)

IdS serveur d'identité (*identity server*)

IdSP fournisseur de service d'identité (*identity service provider*)

PII informations personnellement identifiables (*personally identifiable information*)

PKI infrastructure de clé publique (*public key infrastructure*)

RP partie utilisatrice (*relying party*)

SP fournisseur de services (*service provider*)

XML langage de balisage extensible (*extensible markup language*)

5 Conventions

Néant.

6 Capacités générales

La présente Recommandation définit l'ensemble de capacités ci-après. Les capacités d'utilisateur et les capacités fonctionnelles énoncées dans les paragraphes ci-dessous sont obligatoires, sauf s'il est indiqué qu'elles sont facultatives.

6.1 Capacités d'utilisateur

Les capacités d'utilisateur sont les suivantes:

1) prendre en charge des mécanismes d'authentification mutuelle;
2) fournir une interface d'authentification cohérente, afin de prendre en charge différents mécanismes d'authentification avec le client d'identité numérique (DIC);
3) fournir un sélecteur d'identité permettant à l'utilisateur de choisir le justificatif d'identité qui va être utilisé pour l'authentification. Le choix du justificatif d'identité à utiliser pour l'authentification peut être limité par certaines prescriptions de site web. Dans un souci de commodité pour l'utilisateur, le choix de la méthode d'authentification et du justificatif d'identité associé peut être délégué au fournisseur de service d'identité (possibilité pour l'utilisateur de choisir uniquement un fournisseur de service d'identité mais pas de justificatif d'identité particulier à utiliser pour l'authentification auprès de ce fournisseur de service d'identité);
4) fournir une interface intuitive et cohérente pour gérer avec une sécurité maximale les informations de justificatif d'identité de l'utilisateur;
5) prendre en charge l'inscription ou l'abonnement automatique à un site web, afin de réduire le plus possible l'interaction de l'utilisateur avec le site, tout en laissant à l'utilisateur la pleine maîtrise pour activer et désactiver ces mécanismes. Ceci est facultatif;
6) fournir les informations d'identité chaque fois que l'utilisateur le souhaite et permettre à ce dernier de maîtriser pleinement l'échange d'identité, avec un mécanisme de protection de la confidentialité approprié;
7) mettre à la disposition de l'utilisateur des mises à jour automatiques des informations d'identité partagées, lorsque la source initiale est modifiée sous son autorité;
8) permettre à l'utilisateur d'exercer un contrôle complet sur les modalités d'établissement des politiques de sécurité et de confidentialité et sur les modalités de leur application pour contrôler l'échange d'identité avant le partage des informations d'identité, pour que l'utilisateur puisse avoir une influence directe sur l'établissement d'une politique et sur son application;
9) permettre aux utilisateurs de visionner les détails des informations d'identité qu'ils partagent avec chaque entité;
10) prendre en charge des capacités de gestion de session d'authentification pour éviter à l'utilisateur de se réauthentifier systématiquement auprès d'un fournisseur de service d'identité pour pouvoir accéder aux sites web.

6.2 Capacités fonctionnelles

Les capacités fonctionnelles pour le cadre d'échange d'identité numérique sont définies ci-après. Elles sont requises pour assurer les fonctions minimales nécessaires au cadre d'échange d'identité numérique.

1) prendre en charge la gestion intégrée des justificatifs d'identité permettant de gérer les informations de justificatif d'identité de l'utilisateur pour l'authentification;

2) prendre en charge la gestion des liaisons d'échange d'identité, afin de donner à l'utilisateur une vue d'ensemble complète des entités avec lesquelles il a des connexions pour l'échange d'identité;

3) prendre en charge de multiples mécanismes d'authentification, qui peuvent notamment reposer sur un mot de passe, sur une infrastructure de clés publiques (PKI) ou sur des données biométriques;

4) prendre en charge les mécanismes d'échange d'identité qui permettent d'assurer une liaison bidirectionnelle pour le partage des informations d'identité de l'utilisateur entre entités utilisant un client DIC;

5) prendre en charge les mécanismes de contrat numérique pour établir un contrat aux fins de l'échange d'identité et l'utiliser pour appliquer les politiques de sécurité et de confidentialité pour la diffusion des informations PII;

6) prendre en charge la synchronisation des informations d'identité, pour mettre à jour systématiquement les informations d'identité réparties et partagées lorsque la source des informations d'identité diffusées est modifiée. Les informations d'identité qui nécessitent une synchronisation sont limitées aux informations PII qui sont modifiées directement par un utilisateur;

7) prendre en charge la transformation universelle des jetons afin de rendre le cadre interopérable avec les systèmes actuels de gestion d'identité;

8) faire en sorte que le cadre soit aussi indépendant que possible du processus d'authentification, pour éviter les dépendances entre le client DIC et les mécanismes d'authentification pris en charge au niveau des fournisseurs de service d'identité (ou, au moins, faire en sorte que le cadre puisse facilement prendre en charge tous les mécanismes d'authentification, en particulier ceux qui sont propres aux opérateurs de télécommunication);

9) prendre en charge des mécanismes permettant au fournisseur de service d'identité d'interagir avec l'utilisateur pendant le processus d'authentification, avec la fourniture de sa propre interface d'authentification (interface graphique d'utilisateur (GUI, *graphic user interface*));

10) prendre en charge le stockage des jetons d'identité sur divers supports (clé USB, carte SIM, service de stockage basé sur le réseau, etc.) avec une couche de stockage bien définie à utiliser par le client DIC.

6.3 Lignes directrices de sécurité

Afin de concevoir un cadre DIIF sécurisé, il est recommandé d'appliquer les lignes directrices de sécurité suivantes:

– La sécurité des communications DIIF dépendra du modèle de confiance sous-jacent, qui repose généralement sur l'infrastructure de gestion de clés (par exemple, l'infrastructure PKI ou les clés secrètes).

– Il conviendrait d'utiliser un protocole de sécurité de la couche transport, pour assurer l'intégrité et la confidentialité des données (par exemple, par chiffrement) lorsque le message est transporté par un réseau.

– Les parties qui parviennent à un accord devraient signer numériquement le contrat numérique; à titre facultatif, ce contrat pourra être chiffré si nécessaire.

– Il serait souhaitable de signer numériquement et de chiffrer, lorsqu'elles sont stockées, les données contenant les informations d'identité stockées au niveau du client DIC.

– Etant donné que l'utilisateur est autorisé à déplacer son jeton d'identité d'un dispositif à un autre, une politique permettant de préserver la sécurité des données lorsqu'elles sont en transit est nécessaire.

7 Amélioration du contrôle par l'utilisateur de l'échange d'identité numérique

7.1 Introduction

La fédération d'identité [b-LA-FF] a été mise en œuvre pour connecter les informations d'identité réparties entre le fournisseur de service d'identité (IdSP) et le fournisseur de services (SP). Si le fournisseur de services veut garantir les informations d'authentification émanant d'un fournisseur de service d'identité, il faut qu'il existe une relation de confiance entre les deux parties. Ce domaine de confiance, appelé "cercle de confiance" (CoT), qui peut comprendre un ou plusieurs fournisseurs de service d'identité et fournisseurs de services. Dans un cercle de confiance, si l'utilisateur est authentifié auprès d'un fournisseur de service d'identité, il est autorisé à accéder aux fournisseurs de services du cercle de confiance sans nouvelle authentification. Par conséquent, un utilisateur a besoin de s'authentifier une seule fois dans un cercle de confiance.

Toutefois, le nombre d'authentifications auxquelles un utilisateur doit procéder augmente à mesure que le nombre des cercles de confiance s'accroît. Dans cette situation, il faut qu'un utilisateur s'authentifie auprès du cercle de confiance à chaque visite. Autrement dit, l'utilisateur doit gérer les informations de justificatif d'identité auprès d'un fournisseur de service d'identité dans un cercle de confiance et il n'est pas rare que l'utilisateur oublie le mot de passe ou le mette par écrit, d'où une augmentation du risque de divulgation non autorisée. La fédération au sein d'un cercle de confiance constitue un moyen commode pour échanger les informations d'identité d'un utilisateur. Toutefois, le partage d'informations d'identité entre cercles de confiance nécessite au préalable un accord commercial, ce qui prend généralement beaucoup de temps en raison des formalités juridiques que cela implique. Si le domaine de la gestion d'identité est limité à l'environnement de l'entreprise, la technologie de la fédération constitue une solution possible, rentable et efficace. Si, au contraire, le domaine du système de gestion d'identité (IdM) s'étend à l'Internet, il est difficile de conclure des accords commerciaux entre entreprises pour toutes les fédérations.

Dans les systèmes de gestion d'identité à grande échelle centrés sur l'application, il est possible que des services et politiques d'identité soient conçus pour répondre aux prescriptions des fournisseurs de service d'identité et de services et soient optimisés pour répondre aux prescriptions relatives aux applications, par exemple pour la configuration des informations relatives au compte de l'utilisateur. Lorsqu'un service d'identité est fourni à l'utilisateur, l'échange d'identité a généralement lieu directement entre un fournisseur de service d'identité et un fournisseur de services. Dans ce cas, l'utilisateur dispose d'un contrôle limité sur la diffusion de ses informations d'identité.

Etant donné que les informations d'identité sont échangées entre les entités d'une entreprise sans intervention de l'utilisateur, la protection de la sécurité et de la confidentialité peut être négligée. Un problème se pose lorsque deux entités tentent de partager les informations d'identité d'un utilisateur, qui appartiennent à ce dernier. Etant donné que les deux entités traitent de l'identité de l'utilisateur, il leur faut conclure au préalable un accord commercial et un accord sur la politique de confidentialité. Si une entité doit seulement partager l'identité d'un utilisateur avec le propriétaire d'origine, il suffit que chaque entité conclue un accord et établisse une politique de sécurité et de confidentialité avec le propriétaire en vue de l'utilisation de ses informations d'identité (ou avec l'entité qui gère son identité).

Pour résoudre ce problème, un cadre est défini dans la présente Recommandation, afin d'améliorer le contrôle par l'utilisateur lorsque des informations relatives à l'identité numérique de l'utilisateur sont échangées.

7.2 Menaces pour la sécurité

Si les menaces qui apparaissent dans le cyberespace ne sont pas correctement prises en considération, il est très probable qu'un grand nombre d'entre elles existent dans les systèmes de gestion d'identité (IdM). Les menaces générales en matière de sécurité qui existent dans le cyberespace sont décrites dans la Recommandation [UIT-T X.1205].

Dans les systèmes IdM, diverses menaces pour la sécurité rendent les systèmes vulnérables ou peuvent compromettre leur sécurité et mettre ainsi en danger une organisation. La fraude d'identité est l'une des menaces pour la sécurité les plus courantes dans l'environnement IdM.

La fraude d'identité est un problème de sécurité qui est au premier plan de l'actualité, en particulier pour les organisations qui stockent et gèrent de grandes quantités d'informations personnellement identifiables. Or, non seulement les attaques causant la perte de données personnelles risquent de saper la confiance des clients et des institutions et de nuire gravement à la réputation d'une organisation, mais les violations de données peuvent aussi être financièrement coûteuses pour les organisations. Actuellement, la fraude d'identité peut être déclenchée par l'hameçonnage.

Le hameçonnage consiste, pour une tierce partie, à demander des informations confidentielles à un individu, un groupe ou une organisation, en simulant ou en détournant une marque spécifique, généralement connue, avec comme finalité habituelle, le produit financier. Un site web de hameçonnage est un site conçu pour simuler le site web légitime de l'organisation dont la marque est détournée. Un intrus tente de tromper les utilisateurs en les amenant à révéler des données personnelles, par exemple un numéro de carte de crédit, un justificatif d'identité bancaire en ligne et d'autres informations à caractère sensible, qu'il pourra ensuite utiliser pour commettre des actes frauduleux. Dans les systèmes de gestion d'identité, le hameçonnage représente une grave menace, dans la mesure où les informations d'authentification de la victime, ou d'autres informations personnellement identifiables, peuvent être utilisées, lorsqu'elles sont saisies par un intrus, pour usurper une identité ou commettre d'autres activités frauduleuses.

7.3 Modèle théorique d'échange d'identité numérique

Dans ce modèle théorique, le cadre d'échange d'identité numérique (DIIF) emploie la notion de client d'identité numérique (DIC), qui peut contrôler l'échange d'informations d'identité numérique. Le pouvoir qui est donné à l'utilisateur de contrôler la diffusion des informations d'identité peut permettre de réduire nettement les menaces pour la sécurité qui sont décrites dans le paragraphe intitulé "Menaces pour la sécurité" (voir § 7.2).

La Figure 1 illustre le modèle théorique d'échange d'identité numérique.

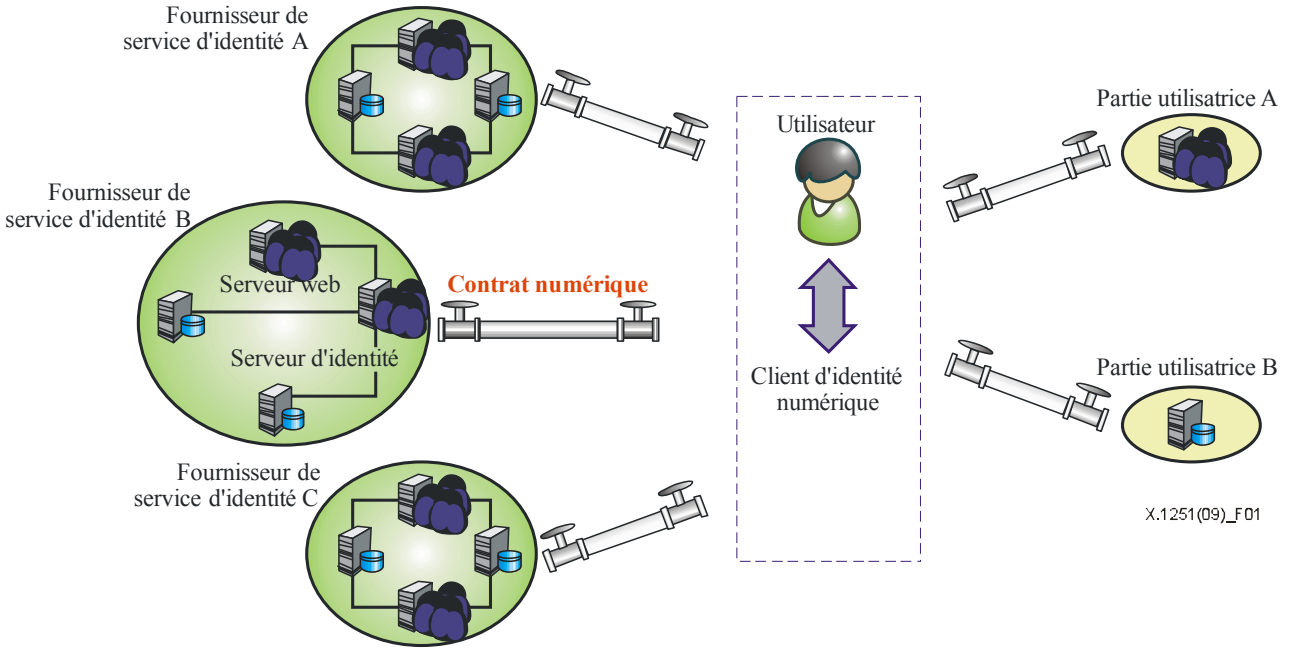

Figure 1 – Modèle théorique d'échange d'identité numérique

7.3.1 Serveur d'identité

Un serveur d'identité (IdS) est le principal serveur qui fournit les informations d'identité de l'utilisateur à l'entité requérante ou demande des informations d'identité à un client d'identité numérique pour des services web. Le serveur IdS peut être un fournisseur de service d'identité, s'il fournit des informations d'identité, sinon il peut s'agir d'une partie utilisatrice (RP) s'il utilise les informations d'identité fournies par l'utilisateur. Un serveur IdS peut jouer à la fois le rôle de fournisseur de service d'identité et celui de partie utilisatrice. Dans ce cas, il fournit ses propres informations d'identité pour certains services web mais demande celles de l'utilisateur pour certains autres. Un serveur web peut demander les informations d'identité d'un utilisateur à un serveur IdS, afin de fournir un service web.

7.3.2 Client d'identité numérique

Le client d'identité numérique (DIC) est un programme qui fournit à l'utilisateur des services d'authentification, de gestion de justificatifs d'identité et de session, d'échange d'identité et de protection de la confidentialité. S'il doit partager des informations d'identité avec le fournisseur de service d'identité ou la partie utilisatrice, le client DIC établit un lien avec le serveur IdS dans un domaine. Le client DIC peut passer un contrat avec le serveur IdS, afin de décrire les termes et conditions régissant le service d'échange d'identité, de manière à améliorer les aspects de confidentialité et de sécurité des informations d'identité échangées. Les informations d'identité de chaque utilisateur passent par le client DIC, de sorte que l'utilisateur en question peut contrôler le partage de ses informations d'identité. En particulier, en fonction des accords conclus entre un utilisateur et une entité, l'utilisateur dispose d'un plein contrôle sur la nature des données d'identité qui sont échangées, sur les finalités, sur les destinataires prévus et sur la durée d'utilisation de ces données. La découverte des informations d'identité de l'utilisateur n'est pas nécessaire, puisque le client dispose de toutes les informations de liaison nécessaires pour la distribution et l'extraction sélectives des informations d'identité.

7.3.3 Fournisseur de service d'identité

Un fournisseur de service d'identité (IdSP) est l'entité qui gère l'identité de l'utilisateur, fournit des services d'authentification et d'autorisation et des services d'échange d'identité pour les serveurs web. Dans le modèle théorique, le rôle de fournisseur de service d'identité peut être attribué à

l'entité qui gère l'identité de l'utilisateur et fournit ces informations lorsque le client DIC les demande. Le fournisseur de service d'identité gère les informations d'identité qui lui sont fournies par l'utilisateur ou celles qu'il génère lui-même.

7.3.4 Partie utilisatrice

Toujours dans le modèle théorique, le rôle de partie utilisatrice (RP) est attribué à l'entité qui demande l'identité de l'utilisateur à un client DIC et fournit un service compte tenu des informations d'identité reçues. La partie utilisatrice n'est pas tributaire du fournisseur de service d'identité pour l'authentification. Un utilisateur recourra au client DIC pour s'authentifier auprès de la partie utilisatrice.

7.3.5 Utilisateur

La définition d'utilisateur est donnée au § 3. Dans le modèle théorique, un utilisateur est généralement une personne ou un abonné dans le contexte de la gestion d'identité centrée sur l'utilisateur. L'utilisateur est l'utilisateur final qui possède et exploite un client DIC.

7.4 Contrat numérique

Les informations personnellement identifiables (PII) qui circulent entre un fournisseur de service d'identité et une partie utilisatrice doivent passer par l'intermédiaire d'un client d'identité numérique, dans un environnement de gestion d'identité centré sur l'utilisateur. Cela permet à l'utilisateur de contrôler l'utilisation de ses informations PII. Un contrat numérique est conclu uniquement entre un utilisateur et un fournisseur de service d'identité ou entre un utilisateur et une partie utilisatrice. Les contrats multipartites ne sont pas autorisés car ils peuvent compliquer les problèmes de gestion auxquels les utilisateurs sont confrontés. Un contrat numérique est le principal élément qui permet à l'utilisateur de contrôler avec précision ses flux d'information PII. La Figure 2 illustre la structure d'un contrat numérique.

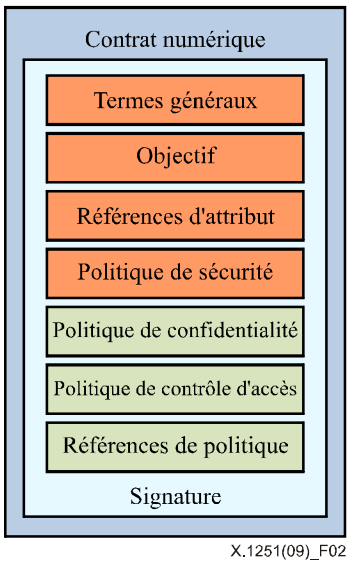

Figure 2 – Structure d'un contrat numérique

Parmi les types de contrôles qui peuvent être définis par des contrats numériques, on peut citer les politiques requises pour faire transiter une relation d'échange d'identité. En fonction des prescriptions réglementaires ou d'autres prescriptions politiques, il se peut que le contrat numérique ne soit pas nécessaire à chaque échange d'identité. Ce contrat n'est nécessaire que lorsque le flux ou la mise en mémoire cache d'informations PII partagées doit être contrôlé. Cet élément est aussi souple et extensible que les contrats réels (par exemple, les accords de non-divulgation). En outre, étant donné que les contrats numériques peuvent eux-mêmes être des documents XML, ils peuvent

régir leurs propres révisions, modifications et suppressions (c'est-à-dire des contrats réels). Les principaux éléments d'un contrat numériques sont les suivants:

1) Termes généraux: décrivent la version, la date de l'accord et la date de la validation ainsi que toute notification destinée à un utilisateur. Cet élément est obligatoire.

2) Objectif: utilisation prévue des informations PII d'un utilisateur. Il s'agit d'un élément obligatoire.

3) Références d'attribut: indiquent à quels attributs de l'entité se réfère le contrat. Cet élément est obligatoire.

4) Politique de sécurité: cet élément doit impérativement contenir la politique d'authentification et de sécurité des informations qui indique comment deux entités peuvent être authentifiées et comment les informations sont sécurisées. Il s'agit d'un élément obligatoire.

5) Politique de confidentialité: cet élément peut contenir tout type de déclaration de politique de confidentialité. La synchronisation et la terminaison des informations PII de l'utilisateur diffusées peuvent y être spécifiées. Il faut garantir la protection de la confidentialité conformément à la législation régionale/nationale applicable en matière de confidentialité. Il s'agit donc d'un élément facultatif.

6) Politique de contrôle d'accès: toute politique de contrôle d'accès ou d'autorisation peut être spécifiée dans cet élément. Il s'agit d'un élément facultatif.

7) Références de politique: les références à des politiques définies à l'extérieur peuvent être spécifiées ici. Il s'agit d'un élément facultatif.

8) Signature: un contrat peut être conclu entre deux entités qui parviennent à un accord sur le contenu du contrat numérique. Il ne peut comporter plus de deux signatures, émanant des deux entités qui acceptent le contrat, comme cela est expliqué au début du présent paragraphe. Le contrat doit être signé par les deux entités en vue de sa validité et de son intégrité. La signature du contrat par l'utilisateur vaut accord. La signature couvre les parties du contrat qui vont des termes généraux aux références de politique (voir la Figure 2). Il s'agit d'un élément obligatoire.

7.5 Trois couches d'échange d'identité

Le présent paragraphe définit trois couches, à savoir: les couches d'application, d'échange d'identité et de communication.

7.5.1 Couche d'application

La couche d'application peut être une application web type qui fonctionne sur l'Internet ou dans un environnement de communication mobile. Un utilisateur utilise par exemple un navigateur web pour demander un service web à un serveur web. Lorsqu'une entité de l'application doit demander une authentification ou un service d'identité, elle appelle le service fourni dans la couche d'échange d'identité. Logiquement, le client DIC est situé à la fois dans la couche d'application et dans la couche d'échange d'identité, reliant les deux couches pour fournir à un utilisateur des services transparents relatifs à l'identité. Chaque fois qu'un utilisateur essaie de se connecter à un site web, il appelle le sélecteur d'identité, qui est une composante du gestionnaire d'interface de l'utilisateur, au niveau du client, afin de choisir un jeton qui représente une identité pour s'authentifier au niveau du site web. Lorsqu'une application web doit partager les informations d'identité de l'utilisateur pour traiter la demande de service de ce dernier, elle peut appeler l'un des services d'échange d'identité fournis dans la couche d'échange d'identité. L'emplacement de la description de service dans la couche d'échange d'identité est fourni pour l'administration de l'application web.

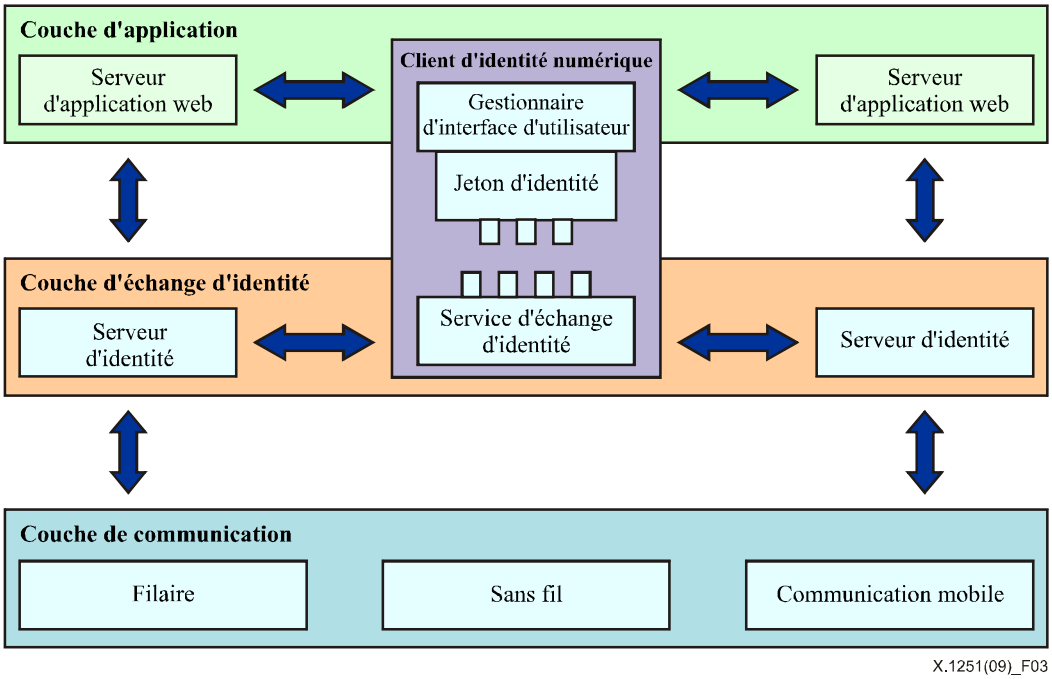

Figure 3 – Couche d'échange d'identité

7.5.2 Couche d'échange d'identité

La couche d'échange d'identité constitue une couche de liaison transparente pour l'échange d'identité, qui vise à faciliter l'échange d'identité entre entités et à permettre à l'utilisateur de maîtriser pleinement l'application de ses politiques de sécurité et de confidentialité.

Grâce à la mise en œuvre de cette couche, le partage des informations d'identité entre différentes entités peut être élaboré et déployé indépendamment de toute application, puisqu'il n'est pas nécessaire qu'une application connaisse le fonctionnement détaillé de l'échange d'identité. En outre, la couche d'échange d'identité peut fournir diverses fonctions relatives à l'échange d'identité aux solutions de gestion d'identité existantes qui ne sont pas dotées de capacités d'échange d'identité. Le paragraphe intitulé "Contrat numérique" décrit en détail comment la couche d'échange d'identité facilite le respect des politiques de sécurité et de confidentialité (voir § 7.4).

7.5.3 Couche de communication

La couche de communication est une couche indépendante qui est chargée du transport des données d'un dispositif à un autre.

8 Cadre régissant l'échange d'identité numérique

8.1 Principes de conception

Ce cadre repose sur les principes de conception suivants, afin d'assurer un échange d'identité transparent entre les entités de l'environnement informatique, notamment l'environnement informatique mobile et ubiquitaire.

- **Indépendant** – Le cadre n'est rattaché à une aucune application ni à aucun environnement de réseau particulier. En d'autres termes, le cadre lui-même doit pouvoir s'adapter, le cas échéant, à tout environnement.

- **Connectable** – Dans un environnement informatique mobile ou ubiquitaire, un utilisateur peut travailler avec plusieurs dispositifs à des fins professionnelles ou pour ses loisirs. En pareil cas, l'utilisateur a besoin d'informations d'identité essentielles, qui permettent d'établir son identité. Ces informations doivent être conçues de manière à pouvoir être intégrées dans n'importe quel dispositif, de sorte que l'utilisateur n'aura qu'à insérer ses informations d'identité dans le dispositif pour pouvoir l'utiliser.
- **Souple** – Le cadre doit être conçu avec la souplesse nécessaire pour pouvoir être intégré dans n'importe quel dispositif, qu'il s'agisse d'un poste de travail ou d'un petit équipement informatique ubiquitaire. Le cadre doit être suffisamment souple pour pouvoir être configuré et s'adapter ainsi à différents environnements informatiques.
- **Modulable** – Le cadre lui-même doit pouvoir fonctionner dans un seul domaine et entre domaines, sans que son intégration dans un système existant n'entraîne une surcharge de communications ou de calculs.

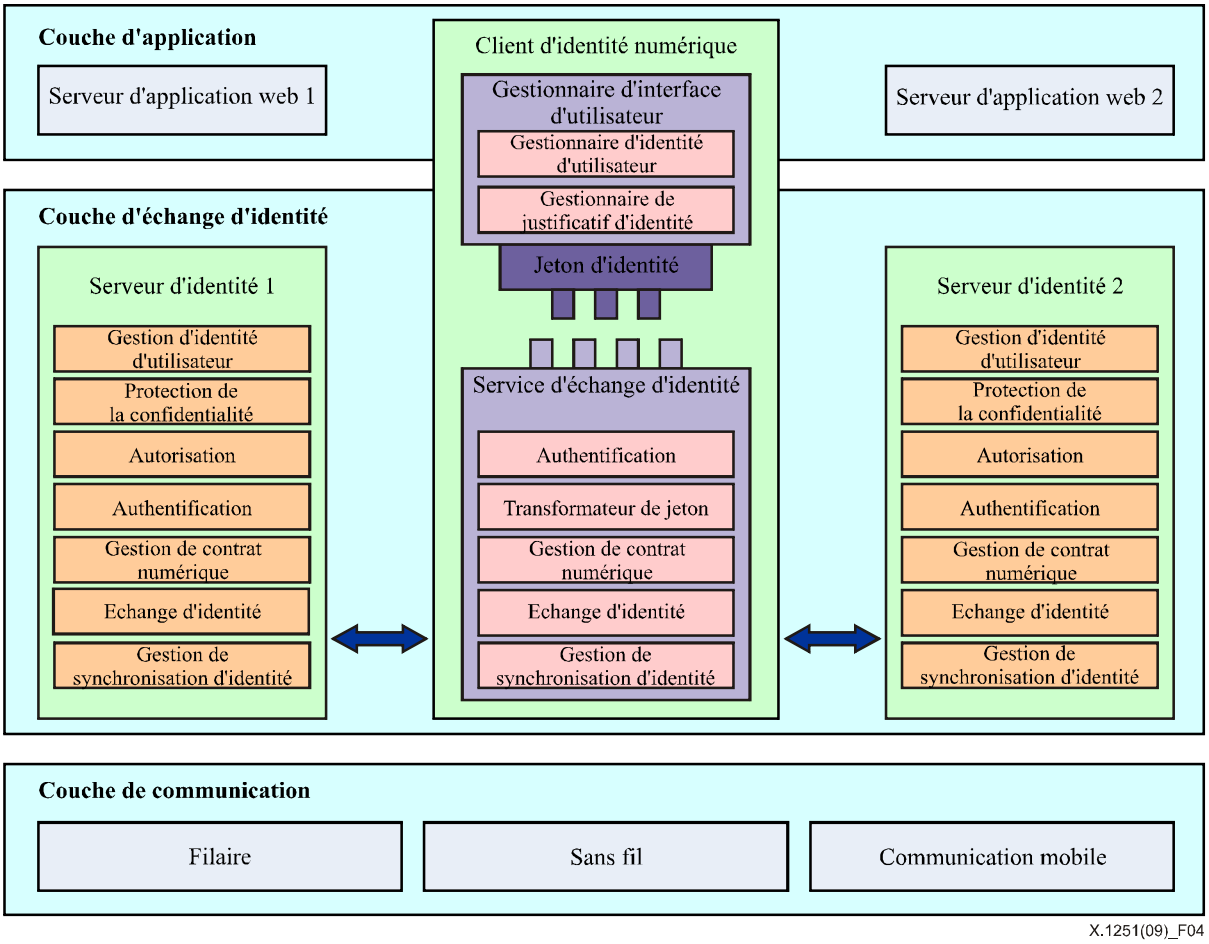

Figure 4 – Cadre régissant l'échange d'identité numérique

8.2 Eléments du cadre

Le client DIC est le principal élément de ce cadre et facilite la liaison d'identité qui connecte tous les fournisseurs de service d'identité de l'utilisateur et les parties utilisatrices. Un utilisateur peut rechercher et mettre à jour ses informations d'identité chaque fois que cela est nécessaire, en utilisant la liaison préétablie.

Le client DIC comprend trois parties: le gestionnaire de l'interface d'utilisateur, le service d'échange d'identité et le jeton d'identité.

La Figure 4 représente les éléments fonctionnels du cadre.

8.2.1 Gestion d'identité d'utilisateur

Il s'agit de l'élément qui gère les informations d'identité de l'utilisateur qui seront partagées par les entités. Au niveau du fournisseur de service d'identité, la gestion d'identité est principalement axée sur le stockage. Par ailleurs, la gestion d'identité au niveau du client DIC essaie de mettre l'accent sur l'interface d'utilisateur graphique qui présente les informations d'identité à l'utilisateur.

8.2.2 Protection de la confidentialité

Il s'agit de l'élément qui gère la fonction relative à la confidentialité chargée de protéger les informations d'identité de l'utilisateur. Cet élément suit les informations d'audit relatives à l'utilisation et à la finalité de l'identité de l'utilisateur. La fonction applique également les contraintes en matière de confidentialité décrites dans un contrat numérique, chaque fois que l'identité de l'utilisateur est utilisée involontairement ou délibérément. Il faut garantir la protection de la confidentialité conformément à la législation régionale/nationale applicable en matière de confidentialité.

8.2.3 Autorisation

Le service d'autorisation est chargé de la prise de décisions concernant les droits d'accès de l'utilisateur et l'application des décisions en matière d'autorisation, en fonction des privilèges de l'utilisateur. L'autorisation est un service facultatif, qui n'est fourni que lorsque l'accès aux ressources doit être contrôlé en fonction des droits de l'utilisateur.

8.2.4 Authentification

Il s'agit de l'élément qui fournit un cadre d'authentification générique prenant en charge différents types de mécanismes d'authentification. Le service d'authentification comprend l'authentification mutuelle pour les clients et les serveurs.

8.2.5 Gestionnaire de contrat numérique

Il s'agit de l'élément qui gère la liste des contrats numériques établis entre l'utilisateur et le fournisseur de service d'identité aux fins de l'authentification, du contrôle d'accès et de la protection de la confidentialité. Le gestionnaire gère la durée de vie d'un contrat numérique qui est signé par signature numérique.

8.2.6 Echange d'identité

Il s'agit de l'élément principal qui assure le service d'échange d'identité. L'échange d'identité se compose de deux services: extraction et mise à jour. Si les informations d'identité sont stockées dans une entité, un client DIC peut en extraire une identité, et inversement. Si ces informations sont modifiées, l'entité peut procéder à la mise à jour ou à la distribution sélective, auprès du client DIC, des informations d'identité modifiées, et inversement. La description plus en détail de cet élément est en dehors du domaine d'application de la présente Recommandation.

8.2.7 Gestionnaire de synchronisation d'identité

Cet élément gère le processus de synchronisation d'identité au niveau du client DIC. Lorsque les informations d'identité stockées par un fournisseur de service d'identité sont modifiées, celui-ci procède à la mise à jour de l'identité modifiée auprès du client DIC. Au niveau du client DIC, cet élément procède à la mise à jour de l'identité dans la fonction d'échange d'identité pour chaque partie utilisatrice avec laquelle le client DIC a partagé l'identité de l'utilisateur. A noter que seule une partie utilisatrice à laquelle le client DIC a déjà distribué sélectivement cette identité peut en recevoir une mise à jour.

8.2.8 Gestionnaire de l'interface d'utilisateur

Il s'agit de l'élément qui présente l'interface graphique d'utilisateur pour les informations d'identité et de justificatif d'identité de l'utilisateur. D'une manière générale, cet élément a une relation étroite avec le serveur d'application web lorsqu'un utilisateur doit se connecter en utilisant l'authentification ou partage ses informations d'identité pour un service.

8.2.9 Gestion de justificatif d'identité

Il s'agit de l'élément qui gère les informations de justificatif d'identité pour l'authentification générées par l'entité ou par le site. Un utilisateur peut avoir plusieurs justificatifs d'identité, par exemple un mot de passe, un certificat X.509 et des données biométriques. Une représentation graphique commune des informations de justificatif d'identité est définie pour que l'expérience des utilisateurs soit homogène.

8.2.10 Jeton d'identité

Un jeton d'identité est un modèle de données de l'identité numérique. Il peut être raccordé à un client d'identité numérique afin de connecter le gestionnaire d'interface d'utilisateur au service d'échange d'identité, pour permettre le fonctionnement du client DIC. La représentation logique du jeton peut être effectuée lorsque le gestionnaire d'interface d'utilisateur est rattaché. Ainsi, lorsqu'un utilisateur commute son environnement de travail depuis un ordinateur personnel vers un téléphone mobile, il lui suffit de transporter le jeton et de le raccorder au téléphone mobile. Le matériel qui contiendra le jeton pourra être une carte à puce, un jeton USB, etc.

8.2.11 Service d'échange d'identité

Il s'agit de la partie service qui est responsable de l'échange et de la synchronisation d'identité. Selon le réseau ou la plate-forme de communication qui est utilisé, cette partie doit être modifiée pour s'intégrer à l'environnement. Ainsi, le module du service d'échange d'identité d'un ordinateur personnel est très différent de celui d'un téléphone mobile.

8.2.12 Transformateur de jeton

Il s'agit de l'élément qui transforme un jeton émis par un autre système IdM existant en jeton pouvant être compris et traité dans le cadre DIIF et de l'élément passerelle qui interfonctionnera avec d'autres systèmes IdM existants, aux fins de l'échange de plusieurs jetons (par exemple, identité et sécurité). Cet élément est facultatif.

Appendice I

Directives d'application de référence concernant un cadre régissant le contrôle par l'utilisateur de l'identité numérique au moyen de la technologie WS-Trust et des cartes d'information

(Le présent Appendice ne fait pas partie intégrante de cette Recommandation)

NOTE – Le présent Appendice fournit à titre d'exemple une mise en correspondance des technologies WS-Trust [b-WS-TRUST] et des cartes d'information [b-IS-INTEROP] avec les capacités visées par cette Recommandation.

I.1 Introduction

Le présent Appendice décrit la manière dont les prescriptions décrites dans cette Recommandation peuvent être satisfaites au moyen des technologies WS-Trust et des cartes d'information décrites dans [b-CARDSPACE].

I.2 Considérations générales

I.2.1 Client d'identité numérique

Le § 7.3.2 décrit "le concept de client d'identité numérique pouvant contrôler l'échange d'identité numérique".

I.2.2 Couche d'échange d'identité

Le § 7.5.2 décrit la "couche d'échange d'identité destinée à faciliter l'échange d'identité entre plusieurs entités et à permettre à une entité d'exercer un contrôle complet pour mettre en application ses politiques de sécurité et de confidentialité".

I.2.3 Spécification WS-Trust

La spécification WS-Trust définit des extensions qui s'appuient sur la spécification WS-Security, en vue de fournir un cadre permettant de demander et d'émettre des jetons de sécurité et d'établir des relations de confiance. Un requérant, agissant généralement au nom d'une entité, envoie un message RST (RequestSecurityToken) à un service de jeton de sécurité (STS), et reçoit en retour une réponse RSTR (RequestSecurityTokenResponse), qui contient généralement un jeton de sécurité. Celui-ci, qui contient un ensemble de déclarations, peut alors être envoyé à un service web comme preuve de l'identité du requérant. A titre facultatif, un message RST peut être envoyé à un service de jeton de sécurité, avec une demande visant à valider ou à annuler un jeton de sécurité émis précédemment. Ces interactions sont illustrées sur la Figure I.1.

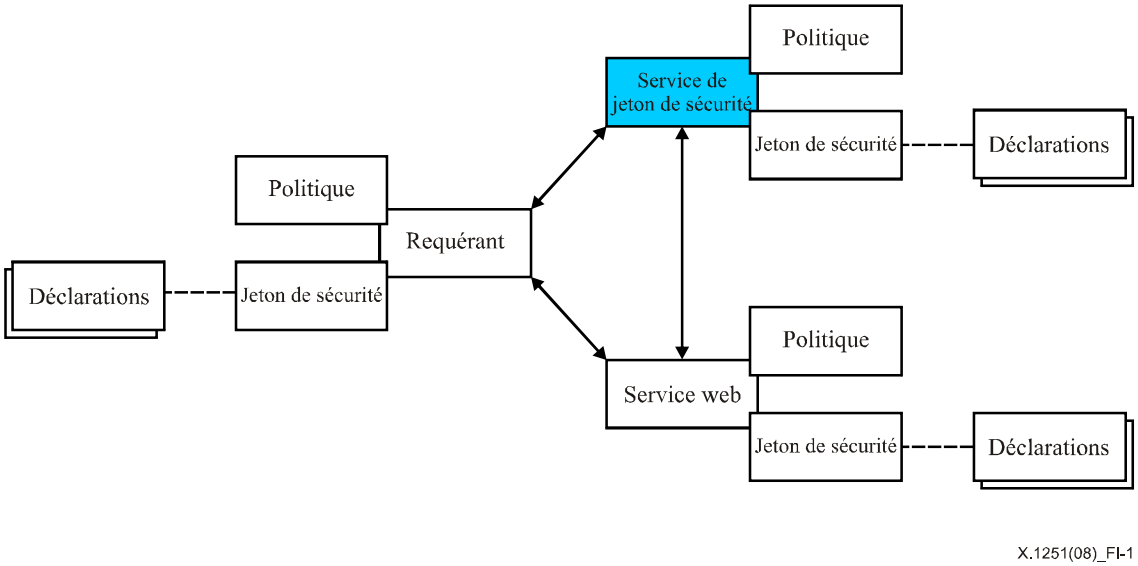

Figure I.1 – Confiance directe WS-Trust

La spécification WS-Trust peut être utilisée pour mettre en œuvre différents modèles autres que le modèle simple de confiance directe. Dans certains cas, un modèle indirect sera utilisé lorsque le service de jeton de sécurité du fournisseur de service d'identité (IP/STS) envoie un message RST à un autre service STS, afin de satisfaire au message RST d'origine, comme indiqué sur la Figure I.2.

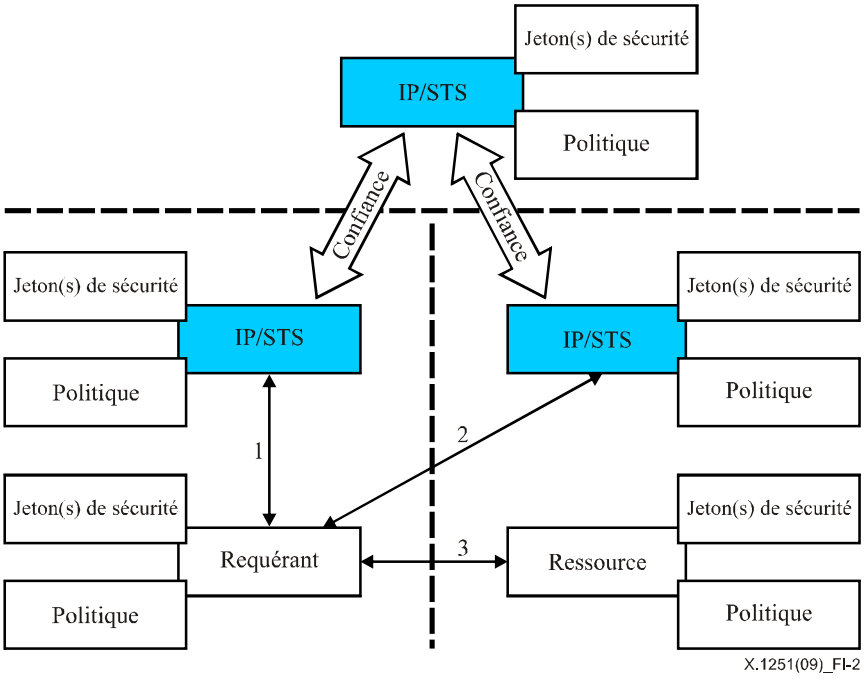

Figure I.2 – Confiance indirecte WS-Trust

I.2.4 Carte d'information

La technologie des cartes d'information est décrite dans le profil d'interopérabilité des sélecteurs d'identité [b-IS-INTEROP]. Grâce à cette technique, un sélecteur d'identité et les éléments associés du système d'identité permettent à des entités de gérer leurs identités numériques à partir de différents fournisseurs de service d'identité et de les employer dans différents contextes pour accéder à des services en ligne.

Lorsque des entités établissent une relation avec des fournisseurs de service d'identité (IdSP), ils reçoivent des cartes d'information; ces cartes contiennent des métadonnées qui décrivent les jetons de sécurité potentiels qui peuvent être demandés par l'intermédiaire de la spécification WS-Trust ainsi que les mécanismes de sécurité utilisés pour protéger et authentifier l'échange de messages. En général, une entité installe ses cartes d'information dans une réserve de cartes accessible à partir de son sélecteur d'identité. La politique de sécurité de la partie utilisatrice est spécifiée par l'intermédiaire de la politique WS-SecurityPolicy [b-WS-SECURITY] et peut être recherchée selon différentes modalités, notamment par intégration dans des pages web. La politique de sécurité spécifie en général des mécanismes définis dans la spécification WS-Security aux fins de l'authentification et de la protection des messages. Le sélecteur d'identité évalue la politique de la partie utilisatrice et l'ensemble de cartes d'information installées dans la réserve de cartes de l'utilisateur et permet à l'entité de choisir parmi la série de cartes d'information celle qui est adaptée (qui permet d'obtenir un jeton de sécurité conforme à la politique). Le sélecteur d'identité demande alors à l'entité des informations d'authentification, le cas échéant, et envoie un message RST au service STS spécifié dans la carte d'information choisie. Le jeton de sécurité obtenu à partir de la réponse RSTR peut alors être joint à un message envoyé à la partie utilisatrice. Si un site web est la partie utilisatrice, le jeton de sécurité peut être posté en réponse au formulaire qui contenait la politique [b-IS-GUIDE].

I.3 Capacités du cadre DIIF

Ce paragraphe traite des capacités du cadre DIIF et décrit la manière dont les technologies WS-Trust et/ou des cartes d'information pourraient être utilisées pour les respecter.

I.3.1 Capacités générales

I.3.1.1 Capacités de l'utilisateur

Le cadre DIIF devrait atteindre les objectifs suivants:

1) *Fournir un sélecteur d'identité permettant à l'utilisateur de choisir le justificatif d'identité qui va être utilisé aux fins de l'authentification*

Le sélecteur d'identité décrit dans la carte d'information offre une expérience d'entité sécurisée, intuitive et cohérente et permet à une entité de choisir des cartes d'information représentant différentes identités fournies par différents fournisseurs IdSP, avec différents mécanismes d'authentification.

2) *Fournir une interface intuitive et cohérente pour gérer avec une sécurité maximale les informations de justificatif d'identité de l'utilisateur*

Le sélecteur d'identité décrit dans la carte d'information offre une expérience d'entité sécurisée, intuitive et cohérente.

3) *Prendre en charge l'inscription ou l'abonnement automatique à un site web, afin de réduire le plus possible l'interaction de l'utilisateur avec le site, tout en laissant à l'utilisateur la pleine maîtrise pour activer et désactiver ces mécanismes. Ceci est facultatif*

Les valeurs de déclaration figurant dans le jeton de sécurité utilisé conjointement avec le sélecteur d'identité décrit dans la carte d'information peuvent fournir des informations qui sont généralement insérées par l'entité au moment de l'enregistrement.

4) *Fournir les informations d'identité chaque fois que l'utilisateur le souhaite et permettre à ce dernier de maîtriser pleinement l'échange d'identité, avec un mécanisme de protection de la confidentialité approprié*

La technologie des cartes d'information repose sur l'hypothèse selon laquelle un fournisseur de service d'identité ne fournira des informations d'identité qu'en réponse à la demande de l'entité. La politique de confidentialité de la partie utilisatrice et du fournisseur de service d'identité est

disponible au niveau de l'interface de l'utilisateur du sélecteur d'identité sécurisé, lors du choix de la carte d'information.

5) *Mettre à la disposition de l'utilisateur des mises à jour automatiques des informations d'identité partagées, lorsque la source initiale est modifiée sous son autorité*

Les valeurs de déclaration figurant dans le jeton de sécurité utilisé conjointement avec le sélecteur d'identité décrit dans la carte d'information peuvent fournir des informations qui sont généralement insérées par l'entité lors de l'enregistrement. Etant donné que les mêmes valeurs de déclaration du jeton de sécurité peuvent être demandées par la partie utilisatrice à chaque visite, les modifications apportées à ces valeurs sont facilement diffusées.

6) *Permettre à l'utilisateur d'exercer un contrôle complet sur les modalités d'établissement des politiques de sécurité et de confidentialité et sur les modalités de leur application pour contrôler l'échange d'identité avant le partage des informations d'identité, pour que l'utilisateur puisse avoir une influence directe sur l'établissement d'une politique et sur son application*

La politique de sécurité de la partie utilisatrice et du fournisseur de service d'identité est disponible au niveau de l'interface sécurisée de l'utilisateur du sélecteur d'identité décrite dans la carte d'information, lors du choix de la carte d'information.

I.3.1.2 Capacités fonctionnelles

1) *Prendre en charge la gestion intégrée des justificatifs d'identité permettant de gérer les informations de justificatif d'identité de l'utilisateur pour l'authentification*

La technologie des cartes d'information comprend un sélecteur d'identité et une interface d'utilisateur de gestion de carte.

2) *Prendre en charge la gestion des liaisons d'échange d'identité, pour donner à l'utilisateur une vue d'ensemble complète des entités avec lesquelles il a des connexions pour l'échange d'identité*

Dans le cas où un jeton de sécurité représentant une session est retourné par un fournisseur de service d'identité, celui-ci peut fournir une interface pour permettre à une entité de visualiser l'ensemble des sessions établies.

3) *Prendre en charge de multiples mécanismes d'authentification, qui peuvent notamment reposer sur un mot de passe, une infrastructure de clés publiques (PKI) ou sur des données biométriques*

Les spécifications WS-Trust et WS-Security offrent un protocole cohérent et intuitif qui prend en charge plusieurs mécanismes d'authentification. Les mises en œuvre des technologies relatives aux cartes d'information fournissent des interfaces API intuitives permettant d'engager le processus d'authentification.

4) *Prendre en charge les mécanismes d'échange d'identité qui permettent d'assurer une liaison bidirectionnelle pour le partage des informations d'identité de l'utilisateur entre entités utilisant un client DIC*

Grâce aux technologies des cartes d'information, le sélecteur d'identité et la réserve de cartes exécutent les fonctionnalités associées à un client DIC.

5) *Prendre en charge les mécanismes de contrat numérique pour établir un contrat aux fins de l'échange d'identité et l'utiliser pour appliquer les politiques de sécurité et de confidentialité pour la diffusion des informations PII*

La politique de sécurité de la partie utilisatrice et du fournisseur de service d'identité est disponible au niveau de l'interface sécurisée de l'utilisateur du sélecteur d'identité décrite dans la carte d'information lors du choix de cette carte.

6) *Prendre en charge la synchronisation des informations d'identité, pour mettre à jour systématiquement les informations d'identité réparties et partagées lorsque la source des informations d'identité diffusées est modifiée. Les informations d'identité qui nécessitent une synchronisation sont limitées aux informations PII qui sont modifiées directement par un utilisateur*

Les valeurs de déclaration figurant dans le jeton de sécurité utilisé conjointement avec le sélecteur d'identité décrit dans la carte d'information peuvent fournir des informations qui sont généralement insérées par l'entité au moment de l'enregistrement. Etant donné que les mêmes valeurs de déclaration du jeton de sécurité peuvent être demandées par la partie utilisatrice à chaque visite, les modifications apportées à ces valeurs peuvent facilement être diffusées.

7) *Prendre en charge la transformation universelle des jetons afin de rendre le cadre interopérable avec les systèmes actuels de gestion d'identité*

La spécification WS-Trust prévoit un mécanisme d'échange de jeton. Le message RST peut comporter un ou plusieurs jetons de sécurité ainsi qu'une indication de l'identité de la partie utilisatrice. La réponse RSTR peut inclure un jeton de sécurité adapté à la partie utilisatrice.

I.3.2 Capacités additionnelles

Le cadre DIIF doit prévoir un mécanisme d'extensibilité pour le sélecteur d'identité et les protocoles connexes, afin de permettre la prise en charge de l'inscription et de la transmission de divers mécanismes d'authentification et des informations relatives à l'assurance.

Ces prescriptions comportent (sans toutefois s'y limiter) la prise en charge de lecteurs de cartes à puce et de dispositifs d'entrée biométriques, ainsi que les formats de données qui leur sont associés, par exemple ceux qui sont décrits dans la norme [b-NIST].

Bibliographie

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

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

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

[b-CARDSPACE] Microsoft (2006), *Introducing Windows CardSpace*.

[b- ETSI 133 980] ETSI TR 133 980 V8.0.0 (2009), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Liberty Alliance and 3GPP security interworking*.

[b-IS-INTEROP] Microsoft (2007), *Identity Selector Interoperability Profile V1.0*.

[b-IS-GUIDE] Microsoft (2007), *A Guide to Using the Identity Selector Interoperability Profile V1.0 within Web Applications and Browsers*.

[b-LA-FF] Liberty Alliance, *Liberty ID-FF Protocols and Schema Specification (ver 1.2)*.

[b-NIST] National Institute of Standards and Technology (2006). *FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors*.

[b-WS-SECURITY] OASIS (2007), *WS-SecurityPolicy 1.2*.

[b-WS-TRUST] OASIS (2007), *WS-Trust 1.3*.

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, 2010