Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1154

(04/2013)

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

Applications et services sécurisés – Protocoles de sécurité

Cadre général de l'authentification combinée dans des environnements à plusieurs fournisseurs de service d'identité

Recommandation UIT-T X.1154

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	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589

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

Recommandation UIT-T X.1154

Cadre général de l'authentification combinée dans des environnements à plusieurs fournisseurs de service d'identité

Résumé

Depuis peu, de nombreux services d'application, en particulier les services financiers, exigent, en raison du nombre accru de vols d'identité, des méthodes d'authentification plus fiables ou des méthodes d'authentification combinée, telles que l'authentification multifacteur. On emploie par exemple des méthodes d'authentification qui reposent sur un mot de passe à usage unique ou d'autres nouvelles méthodes d'authentification plutôt que l'authentification classique au moyen d'un mot de passe.

L'association de méthodes d'authentification permet à plusieurs fournisseurs de service d'identité (IdSP) de mieux garantir l'authentification. La Recommandation UIT-T X.1154 définit, à l'intention d'un fournisseur de services, le cadre général de l'authentification combinée dans des environnements multifournisseurs IdSP. Dans cette Recommandation, trois types de méthodes d'authentification combinée sont examinés: l'authentification multifacteur, l'authentification multiméthode et les authentifications multiples.

Le cadre de cette Recommandation définit des modèles, des opérations de base et des exigences de sécurité pour chaque composante du modèle et pour chaque message échangé entre les composantes du modèle en vue de maintenir un niveau global de garantie d'authentification dans des situations où interviennent plusieurs fournisseurs IdSP.

En outre, ce cadre définit aussi des modèles, des opérations de base et des exigences de sécurité en vue de prendre en charge le service d'authentification qui gère plusieurs fournisseurs IdSP.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1154	2013-04-26	17

Mots clés

Authentification des entités, authentification combinée, authentification multifacteur.

AVANT-PROPOS

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

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

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

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

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

TABLE DES MATIÈRES

Introduction

Depuis peu, de nombreux services d'application, en particulier les services financiers, exigent, en raison du nombre accru de vols d'identité, des méthodes d'authentification plus fiables ou des méthodes d'authentification combinée, telles que l'authentification multifacteur. On emploie par exemple des méthodes d'authentification qui reposent sur un mot de passe à usage unique ou d'autres nouvelles méthodes d'authentification plutôt que l'authentification classique au moyen d'un mot de passe.

Les Recommandations UIT-T traitant de l'authentification en vue de garantir des services d'application sécurisés (voir les références [b-UIT-T X.509] et [b-UIT-T X.1141]) sont des cadres d'authentification normalisés. Dans ces Recommandations UIT-T, on considère avant tout qu'un fournisseur de services et/ou un utilisateur appartiennent à un domaine de sécurité relevant d'un fournisseur IdSP, même si le fournisseur de services et l'utilisateur appartiennent à des domaines de sécurité différents. Afin de renforcer l'authentification, le fournisseur IdSP exige la mise en œuvre de méthodes d'authentification plus fortes (par exemple, celles qui sont décrites dans les références [b-UIT-T X.1151], [b-UIT-T X.1084], [b-UIT-T X.1086] et [b-UIT-T X.1089]).

Par ailleurs, il n'est pas rare qu'un utilisateur obtienne plusieurs identités auprès de plusieurs fournisseurs IdSP et qu'un fournisseur de services établisse des relations de confiance avec plusieurs fournisseurs IdSP. Dans ces environnements multifournisseurs IdSP, le fournisseur de services peut disposer d'un autre moyen pour renforcer l'authentification en faisant appel à plusieurs fournisseurs IdSP pour authentifier l'utilisateur.

En outre, même si le fournisseur de services emploie une authentification plus forte, il peut faire appel à un fournisseur relais de service d'identité pour associer plusieurs fournisseurs IdSP.

Toutefois, puisque chaque fournisseur IdSP est utilisé par différents fournisseurs, une simple association de plusieurs fournisseurs IdSP peut conduire à l'effondrement du niveau général de l'authentification.

Par conséquent, le cadre général doit définir des modèles, des opérations de base et des exigences de sécurité pour chaque composante du modèle et pour chaque message échangé entre les composantes du modèle en vue de maintenir un niveau global de garantie d'authentification dans des situations où interviennent plusieurs fournisseurs IdSP.

De plus, la nécessité de disposer d'une authentification plus forte/plus fiable augmente la complexité de la mise en œuvre et/ou de la gestion du système d'authentification. Par conséquent, on utilise un service d'authentification qui gère l'association de plusieurs fournisseurs IdSP pour authentifier l'utilisateur au nom du service d'application. Ce service d'authentification doit pouvoir gérer plusieurs fournisseurs IdSP qui sont conformes aux politiques d'authentification de chaque service d'application.

Le cadre doit aussi définir des modèles, des opérations de base et des exigences de sécurité en vue de prendre en charge le service d'authentification.

Recommandation UIT-T X.1154

Cadre général de l'authentification combinée dans des environnements à plusieurs fournisseurs de service d'identité

1 Domaine d'application

La présente Recommandation définit le cadre général de l'authentification combinée dans des environnements à plusieurs fournisseurs de service d'identité, qui doit permettre au fournisseur de services d'employer une authentification combinée telle que l'authentification multifacteur.

Le cadre dans la présente Recommandation définit des modèles, des opérations de base et des exigences de sécurité pour chaque composante du modèle et pour chaque message échangé entre les composantes du modèle en vue de maintenir un niveau global de garantie d'authentification dans des situations où interviennent plusieurs fournisseurs IdSP.

En outre, ce cadre définit aussi des modèles, des opérations de base et des exigences de sécurité en vue de prendre en charge le service d'authentification qui gère plusieurs fournisseurs IdSP.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

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

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

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

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

3.1.2 niveau de garantie [b-UIT-T X.1252]: niveau de confiance dans le lien entre une entité et l'information d'identité présentée.

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

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

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

3.1.5 utilisateur final [UIT-T X.1141]: une personne physique qui emploie des ressources pour les besoins d'une application.

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

3.1.7 identité [b-UIT-T X.1252]: représentation d'une entité sous la forme d'un ou de plusieurs attributs qui sont suffisants pour pouvoir distinguer les entités dans un contexte. Aux fins de la gestion des identités (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.

3.1.8 fournisseur relais de service d'identité [b-UIT-T X.1252]: fournisseur de service d'identité faisant office d'intermédiaire digne de confiance entre d'autres fournisseurs de service d'identité.

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

3.1.10 partie utilisatrice [UIT-T X.1141]: entité du système qui décide d'exécuter une action sur la base d'informations provenant d'une autre entité du système. Par exemple, une partie utilisatrice SAML dépend des assertions qu'elle reçoit d'une partie émettrice d'assertions (une autorité SAML) concernant un sujet.

3.1.11 fournisseur de services [UIT-T X.1141]: rôle joué par une entité du système, dans lequel celle-ci fournit des services aux entités principales du système ou à d'autres entités du système.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 facteur d'authentification: type de justificatif d'identité. Il existe trois types de facteurs d'authentification: les facteurs liés à la possession, les facteurs liés à la connaissance et les facteurs biométriques.

3.2.2 facteur biométrique: facteur d'authentification qui permet de vérifier ce que l'entité est ou fait.

3.2.3 authentification combinée: authentification qui utilise plusieurs justificatifs d'identité.

3.2.4 niveau de garantie en vigueur: niveau de garantie d'authentification d'une entité donnée au moment considéré.

3.2.5 facteur lié à la connaissance: facteur d'authentification qui permet de vérifier quelque chose que l'utilisateur connaît.

3.2.6 authentification multifacteur: authentification qui utilise plusieurs justificatifs d'identité provenant d'au moins deux des trois catégories de facteurs d'authentification.

3.2.7 authentification multiméthode: authentification qui utilise plusieurs justificatifs d'identité provenant de différentes méthodes d'authentification.

3.2.8 authentification multiple: authentification qui utilise plusieurs justificatifs d'identité provenant des mêmes méthodes d'authentification.

3.2.9 facteur lié à la possession: facteur d'authentification qui permet de vérifier quelque chose que l'utilisateur possède.

3.2.10 niveau de garantie fourni: niveau de garantie que certains fournisseurs de service d'identité (IdSP) fourniront lorsqu'ils authentifient l'utilisateur.

3.2.11 niveau de garantie requis: niveau de garantie qu'un certain fournisseur de services exigera pour fournir son propre service.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et les acronymes suivants:

ID identité (*identity*)

IdM gestion des identités (*identity management*)

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

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

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

SP fournisseur de services (*service provider*)

5 Conventions

Dans la présente Recommandation:

L'expression "est obligatoire" indique une spécification qui doit rigoureusement être respectée et par rapport à laquelle aucun écart n'est admis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "est recommandé" indique une spécification qui est recommandée mais n'est pas requise de façon absolue. Il ne doit donc pas nécessairement être satisfait à cette spécification pour déclarer la conformité.

L'expression "est interdit" indique une spécification qui doit rigoureusement être respectée et par rapport à laquelle aucun écart n'est admis pour pouvoir déclarer la conformité à la présente Recommandation.

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

6 Types d'authentification combinée

La présente Recommandation comporte les trois types de méthodes d'authentification combinée ci-après:

– L'authentification multifacteur qui utilise plusieurs justificatifs d'identité provenant d'au moins deux des trois catégories de facteurs d'authentification. Par exemple, 1) l'authentification au moyen d'un certificat de clé publique enregistré sur une carte à puce; 2) l'authentification au moyen d'un mot de passe à usage unique, qui utilise un équipement matériel; et 3) l'authentification associant l'authentification au moyen d'un mot de passe à usage unique et l'authentification biométrique, sont des exemples d'authentification multifacteur.

– L'authentification multiméthode qui utilise plusieurs justificatifs d'identité provenant de différentes méthodes d'authentification. Par exemple, 1) l'authentification associant l'authentification au moyen d'un mot de passe à usage unique et l'authentification au moyen d'une phrase de passe; et 2) l'authentification associant l'authentification au moyen

d'empreintes digitales et l'authentification au moyen des veines d'un doigt, sont des exemples d'authentification multiméthode.

– Les authentifications multiples qui utilisent plusieurs justificatifs d'identité provenant des mêmes méthodes d'authentification. Par exemple, 1) l'authentification à double mot de passe; et 2) l'authentification au moyen d'empreintes digitales de plusieurs doigts, sont des exemples d'authentification multiple.

La différence entre les trois méthodes d'authentification susmentionnées est l'association des justificatifs d'identité. Par ailleurs, le "facteur d'authentification" permet de classer les justificatifs d'identité. En outre, il existe trois types de facteurs d'authentification: les facteurs liés à la possession, les facteurs liés à la connaissance et les facteurs biométriques.

– Le facteur lié à la possession est un facteur d'authentification qui permet de vérifier quelque chose que l'utilisateur possède. Il peut s'agir par exemple d'une carte à puce, d'un jeton de sécurité, d'un jeton logiciel, d'un téléphone fixe ou d'un téléphone mobile.
– Le facteur lié à la connaissance est un facteur d'authentification qui permet de vérifier quelque chose que l'utilisateur connaît. Il peut s'agir par exemple d'un mode de passe, d'une phrase de passe ou d'un numéro d'identification personnel (PIN).
– Le facteur biométrique est un facteur d'authentification qui permet de vérifier ce que l'entité est ou fait. Il peut s'agir par exemple d'empreintes digitales, de veines d'un doigt ou de l'iris.

7 Modèles d'authentification dans des environnements à plusieurs fournisseurs de service d'identité

7.1 Modèles de base du point de vue du fournisseur de services

Dans le modèle d'authentification du point de vue du fournisseur de services, il devrait être tenu compte des facteurs suivants, lorsqu'un utilisateur reçoit un service d'application:

– La méthode d'authentification fournie par le fournisseur IdSP est-elle une authentification à facteur unique ou une authentification combinée?
– Le modèle prévoit-il un seul fournisseur IdSP ou plusieurs fournisseurs IdSP? Si le modèle prévoit plusieurs fournisseurs IdSP, ceux-ci fournissent-ils la même méthode ou des méthodes différentes? Si plusieurs fournisseurs IdSP fournissent des méthodes différentes, celles-ci emploient-elles des facteurs différents ou le même facteur?

  Donc l'authentification combinée peut se faire selon huit types de modèles fonctionnels, en fonction du nombre de fournisseurs de services et de fournisseurs IdSP, et un type d'authentification combinée (Tableau 1). En outre, lorsqu'il y a plusieurs utilisateurs dans des environnements multifournisseurs IdSP, il se peut qu'un utilisateur n'ait pas une relation de confiance avec tous les fournisseurs IdSP. En conséquence, il est possible de regrouper les fournisseurs IdSP en fonction du groupe d'utilisateurs avec lesquels ils ont une relation de confiance (Figure 1). Dans ce cas, le facteur suivant est également pris en considération:
– Les fournisseurs IdSP sont-ils classés, du point de vue de la relation de confiance qu'ils ont avec les utilisateurs, en un seul groupe ou en plusieurs groupes?

Si les fournisseurs IdSP sont classés en un seul groupe, les modèles T-3 à T-8 du Tableau 1 peuvent être appliqués.

Si les fournisseurs IdSP sont classés en plusieurs groupes, les modèles T-9 à T-14 peuvent être envisagés (voir le Tableau 2).

Tableau 1 – Modèles d'authentification de base (lorsque les fournisseurs IdSP forment un seul groupe)

	Nombre de fournisseurs IdSP	Nombre de types de méthode d'authentification	Type de la méthode d'authentification fournie par un fournisseur IdSP	Nombre de groupes de fournisseurs IdSP	Méthode d'authentification fournie par un groupe de fournisseurs IdSP
T-1	Un	Un	A facteur unique	Un	Aucune
T-2			Combinée	Un	Combinée (Note 1)
T-3	Plusieurs	Un	A facteur unique	Un	Multiple
T-4			Combinée	Un	Combinée (Note 1)
T-5		Plusieurs (différentes méthodes)	A facteur unique	Un	Multiple, multiméthode (Note 2)
T-6			Combinée (multiple ou multiméthode)	Un	Multiple, multiméthode (Note 3)
T-7		Plusieurs (différents facteurs)	A facteur unique	Un	Multiple, multiméthode, multifacteur (Note 2)
T-8			Combinée	Un	Combinée (Note 3)

NOTE 1 – Les trois types d'authentification combinée peuvent être fournis. Toutefois, la méthode d'authentification fournie dépend du type de l'authentification fournie par le fournisseur IdSP.

NOTE 2 − Les trois types d'authentification combinée peuvent être fournis. Toutefois, la méthode d'authentification fournie dépend du choix des fournisseurs IdSP.

NOTE 3 − Les trois types d'authentification combinée peuvent être fournis. Toutefois, la méthode d'authentification fournie dépend non seulement des types d'authentification fournis par les fournisseurs IdSP mais aussi du choix des fournisseurs IdSP.

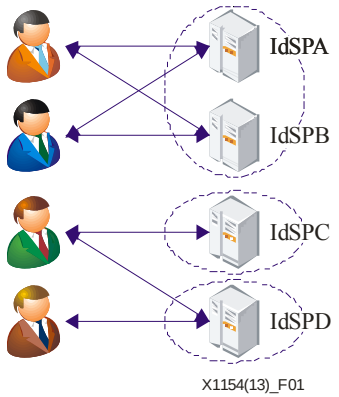

Figure 1 – Exemple de regroupements de fournisseurs IdSP en fonction des relations de confiance avec les utilisateurs

Tableau 2 – Modèles d'authentification de base (lorsque les fournisseurs IdSP sont classés en plusieurs groupes)

	Nombre de fournisseurs IdSP	Nombre de types de méthode d'authentification	Type de la méthode d'authentification fournie par le fournisseur IdSP	Nombre de groupes de fournisseurs IdSP	Méthode d'authentification fournie par un groupe de fournisseurs IdSP
T-9	Plusieurs	Un	A facteur unique	Plusieurs	Multiple
T-10			Combinée	Plusieurs	Combinée (Note 1)
T-11		Plusieurs (différentes méthodes)	A facteur unique	Plusieurs	Multiple, multiméthode (Note 2)
T-12			Combinée (multiple ou multiméthode)	Un	Multiple, multiméthode (Note 3)
T-13		Plusieurs (différents facteurs)	A facteur unique	Plusieurs	Multiple, multiméthode, multifacteur (Note 2)
T-14			Combinée	Plusieurs	Combinée (Note 3)

NOTE 1 – Les trois types d'authentification combinée peuvent être fournis. Toutefois, la méthode d'authentification fournie dépend du type d'authentification fournie par un fournisseur IdSP.

NOTE 2 − Les trois types d'authentification combinée peuvent être fournis. Toutefois, la méthode d'authentification fournie dépend du choix des fournisseurs IdSP.

NOTE 3 − Les trois types d'authentification combinée peuvent être fournis. Toutefois, la méthode d'authentification fournie dépend non seulement des types d'authentification fournis par les fournisseurs IdSP mais aussi du choix des fournisseurs IdSP.

7.1.1 Modèle T-1

Dans le modèle T-1, un fournisseur IdSP fournit une authentification à facteur unique, et un fournisseur IdSP, un fournisseur de services et un ou plusieurs terminaux sont connectés entre eux par l'intermédiaire du réseau.

Lorsque le fournisseur de services reçoit une demande de service émanant du terminal, il demande au fournisseur IdSP d'authentifier l'utilisateur. Le fournisseur IdSP, qui reçoit la demande d'authentification émanant du fournisseur de services, authentifie l'utilisateur au moyen d'une méthode d'authentification à facteur unique. Si les résultats d'authentification reçus du fournisseur IdSP indiquent que l'utilisateur a été authentifié correctement, le fournisseur de services fournit son service au terminal.

Ce modèle ne permet pas de fournir une authentification combinée. Par conséquent, il sort du cadre de la présente Recommandation.

7.1.2 Modèle T-2

Dans le modèle T-2, un fournisseur IdSP fournit une authentification combinée (authentification multiple, multiméthode ou multifacteur), et un fournisseur IdSP, un fournisseur de services et un ou plusieurs terminaux sont connectés entre eux par l'intermédiaire du réseau.

Lorsque le fournisseur de services reçoit une demande de service émanant du terminal, il demande au fournisseur IdSP d'authentifier l'utilisateur. Le fournisseur IdSP, qui reçoit la demande d'authentification émanant du fournisseur de services, authentifie l'utilisateur au moyen d'une méthode d'authentification combinée. Si les résultats d'authentification reçus du fournisseur IdSP

indiquent que l'utilisateur a été authentifié correctement, le fournisseur de services fournit son service au terminal.

Ce modèle permet de fournir tous les types de méthode d'authentification combinée, bien qu'il dépende du type de la méthode d'authentification fournie par le fournisseur IdSP.

7.1.3 Modèle T-3

Dans le modèle T-3, plusieurs fournisseurs IdSP fournissent la même méthode d'authentification à facteur unique, et plusieurs fournisseurs IdSP, un fournisseur de services et un ou plusieurs terminaux sont connectés entre eux par l'intermédiaire du réseau. Et en particulier, dans ce modèle, tous les utilisateurs ont des relations de confiance avec tous les fournisseurs IdSP.

Lorsque le fournisseur de services reçoit une demande de service émanant du terminal, il choisit plusieurs fournisseurs IdSP en vue de satisfaire à la garantie d'authentification requise et demande à chacun des fournisseurs IdSP choisis d'authentifier l'utilisateur. Si tous les résultats d'authentification reçus des fournisseurs IdSP indiquent que l'utilisateur a été authentifié correctement, le fournisseur de services fournit son service au terminal.

Ce modèle permet de fournir une méthode d'authentification multiple.

Il convient de noter que ce modèle permet de fournir une authentification à facteur unique si la méthode d'authentification fournie par un fournisseur IdSP permet de satisfaire à la garantie d'authentification requise. Toutefois, l'authentification à facteur unique dans ce modèle sort du cadre de la présente Recommandation.

7.1.4 Modèle T-4

Dans le modèle T-4, plusieurs fournisseurs IdSP fournissent la même méthode d'authentification combinée, et plusieurs fournisseurs IdSP, un fournisseur de services et un ou plusieurs terminaux sont connectés entre eux par l'intermédiaire du réseau. Et en particulier, dans ce modèle, tous les utilisateurs ont des relations de confiance avec tous les fournisseurs IdSP.

Lorsque le fournisseur de services reçoit une demande de service émanant du terminal, il choisit un ou plusieurs fournisseurs IdSP en vue de satisfaire à la garantie d'authentification requise et demande à chacun des fournisseurs IdSP choisis d'authentifier l'utilisateur. Si tous les résultats d'authentification reçus du ou des fournisseurs IdSP indiquent que l'utilisateur a été authentifié correctement, le fournisseur de services fournit son service au terminal.

Ce modèle permet de fournir tous les types d'authentification combinée, bien qu'il dépende du type de la méthode d'authentification combinée fournie par le fournisseur IdSP et/ou du choix des fournisseurs IdSP. (Des authentifications multifacteurs multiples et des authentifications multiméthodes multiples peuvent être effectuées.)

7.1.5 Modèle T-5

Dans le modèle T-5, plusieurs fournisseurs IdSP fournissent des méthodes d'authentification unique, qui sont de types différents mais emploient le même facteur, et plusieurs fournisseurs IdSP, un fournisseur de services et un ou plusieurs terminaux sont connectés entre eux par l'intermédiaire du réseau. Et en particulier, dans ce modèle, tous les utilisateurs ont des relations de confiance avec tous les fournisseurs IdSP.

Lorsque le fournisseur de services reçoit une demande de service émanant du terminal, il choisit plusieurs fournisseurs IdSP en vue de satisfaire à la garantie d'authentification requise et demande à chacun des fournisseurs IdSP choisis d'authentifier l'utilisateur. Si tous les résultats d'authentification reçus des fournisseurs IdSP indiquent que l'utilisateur a été authentifié correctement, le fournisseur de services fournit son service au terminal.

Ce modèle permet de fournir une authentification multiple ou une authentification multiméthode. Il convient de noter que la méthode d'authentification employée dépend du groupe de fournisseurs IdSP.

Ce modèle permet aussi de fournir une authentification à facteur unique si la méthode d'authentification fournie par un fournisseur IdSP permet de satisfaire à la garantie d'authentification requise. Toutefois, l'authentification à facteur unique dans ce modèle sort du cadre de la présente Recommandation.

7.1.6 Modèle T-6

Dans le modèle T-6, plusieurs fournisseurs IdSP fournissent des méthodes d'authentification combinée, qui sont de types différents mais emploient le même facteur (c'est-à-dire des méthodes d'authentification multiple ou multiméthode), et plusieurs fournisseurs IdSP, un fournisseur de services et un ou plusieurs terminaux sont connectés entre eux par l'intermédiaire du réseau. Et en particulier, dans ce modèle, tous les utilisateurs ont des relations de confiance avec tous les fournisseurs IdSP.

Lorsque le fournisseur de services reçoit une demande de service émanant du terminal, il choisit un ou plusieurs fournisseurs IdSP en vue de satisfaire à la garantie d'authentification requise et demande à chacun des fournisseurs IdSP choisis d'authentifier l'utilisateur. Si tous les résultats d'authentification reçus du ou des fournisseurs IdSP indiquent que l'utilisateur a été authentifié correctement, le fournisseur de services fournit son service au terminal.

Ce modèle permet de fournir des authentifications multiples ou des authentifications multiméthodes, bien qu'il dépende du choix et de l'association des fournisseurs IdSP.

7.1.7 Modèle T-7

Dans le modèle T-7, plusieurs fournisseurs IdSP fournissent des méthodes d'authentification unique, qui emploient différents facteurs, et plusieurs fournisseurs IdSP, un fournisseur de services et un ou plusieurs terminaux sont connectés entre eux par l'intermédiaire du réseau. Et en particulier, dans ce modèle, tous les utilisateurs ont des relations de confiance avec tous les fournisseurs IdSP.

Lorsque le fournisseur de services reçoit une demande de service émanant du terminal, il choisit plusieurs fournisseurs IdSP en vue de satisfaire à la garantie d'authentification requise et demande à chacun des fournisseurs IdSP choisis d'authentifier l'utilisateur. Si tous les résultats d'authentification reçus des fournisseurs IdSP indiquent que l'utilisateur a été authentifié correctement, le fournisseur de services fournit son service au terminal.

Ce modèle permet de fournir tous les types d'authentification combinée. Il convient de noter que la méthode d'authentification employée dépend du choix des fournisseurs IdSP.

Ce modèle permet aussi de fournir une authentification à facteur unique si la méthode d'authentification fournie par un fournisseur IdSP permet de satisfaire à la garantie d'authentification requise. Toutefois, l'authentification à facteur unique dans ce modèle sort du cadre de la présente Recommandation.

7.1.8 Modèle T-8

Dans le modèle T-8, plusieurs fournisseurs IdSP fournissent des méthodes d'authentification combinée, qui emploient différents facteurs, et plusieurs fournisseurs IdSP, un fournisseur de services et un ou plusieurs terminaux sont connectés entre eux par l'intermédiaire du réseau. Et en particulier, dans ce modèle, tous les utilisateurs ont des relations de confiance avec tous les fournisseurs IdSP.

Lorsque le fournisseur de services reçoit une demande de service émanant du terminal, il choisit un ou plusieurs fournisseurs IdSP en vue de satisfaire à la garantie d'authentification requise et demande à chacun des fournisseurs IdSP choisis d'authentifier l'utilisateur. Si tous les résultats

d'authentification reçus du ou des fournisseurs IdSP indiquent que l'utilisateur a été authentifié correctement, le fournisseur de services fournit son service au terminal.

Ce modèle permet de fournir tous les types d'authentification combinée.

7.1.9 Modèle T-9

Dans le modèle T-9, plusieurs fournisseurs IdSP fournissent la même méthode d'authentification à facteur unique, et plusieurs fournisseurs IdSP, un fournisseur de services et plusieurs terminaux sont connectés entre eux par l'intermédiaire du réseau. Et en particulier, dans ce modèle, un ou plusieurs utilisateurs n'ont pas de relation de confiance avec tous les fournisseurs IdSP.

NOTE – Il se peut que, dans ce modèle, un fournisseur IdSP n'ait de relation de confiance avec aucun des utilisateurs. Ce cas de figure sort toutefois du cadre de la présente Recommandation.

Lorsque le fournisseur de services reçoit une demande de service émanant du terminal, il choisit, en vue de satisfaire à la garantie d'authentification requise, plusieurs fournisseurs IdSP dans un groupe de fournisseurs IdSP qui ont des relations de confiance avec l'utilisateur, et demande à chacun des fournisseurs IdSP choisis d'authentifier l'utilisateur. Si tous les résultats d'authentification reçus des fournisseurs IdSP indiquent que l'utilisateur a été authentifié correctement, le fournisseur de services fournit son service au terminal.

Ce modèle permet de fournir une méthode d'authentification multiple.

Il convient de noter que ce modèle permet de fournir une authentification à facteur unique si la méthode d'authentification fournie par un fournisseur IdSP permet de satisfaire à la garantie d'authentification requise. Toutefois, l'authentification à facteur unique dans ce modèle sort du cadre de la présente Recommandation.

7.1.10 Modèle T-10

Dans le modèle T-10, plusieurs fournisseurs IdSP fournissent la même méthode d'authentification combinée, et plusieurs fournisseurs IdSP, un fournisseur de services et plusieurs terminaux sont connectés entre eux par l'intermédiaire du réseau. Et en particulier, dans ce modèle, un ou plusieurs utilisateurs n'ont pas de relation de confiance avec tous les fournisseurs IdSP.

NOTE – Il se peut que, dans ce modèle, un fournisseur IdSP n'ait de relation de confiance avec aucun des utilisateurs. Ce cas de figure sort toutefois du cadre de la présente Recommandation.

Lorsque le fournisseur de services reçoit une demande de service émanant du terminal, il choisit un ou plusieurs fournisseurs IdSP en vue de satisfaire à la garantie d'authentification requise, et demande à chacun des fournisseurs IdSP choisis d'authentifier l'utilisateur. Si tous les résultats d'authentification reçus du ou des fournisseurs IdSP indiquent que l'utilisateur a été authentifié correctement, le fournisseur de services fournit son service au terminal.

Ce modèle permet de fournir tous les types d'authentification combinée, bien qu'il dépende du type d'authentification combinée fournie par le fournisseur IdSP et/ou du choix des fournisseurs IdSP. Des authentifications multifacteurs multiples et des authentifications multiméthodes multiples peuvent être effectuées.

7.1.11 Modèle T-11

Dans le modèle T-11, plusieurs fournisseurs IdSP fournissent des méthodes d'authentification unique, qui sont de types différents mais emploient le même facteur, et plusieurs fournisseurs IdSP, un fournisseur de services et plusieurs terminaux sont connectés entre eux par l'intermédiaire du réseau. Et en particulier, dans ce modèle, un ou plusieurs utilisateurs n'ont pas de relation de confiance avec tous les fournisseurs IdSP.

NOTE – Il se peut que, dans ce modèle, un fournisseur IdSP n'ait de relation de confiance avec aucun des utilisateurs. Ce cas de figure sort toutefois du cadre de la présente Recommandation.

Lorsque le fournisseur de services reçoit une demande de service émanant du terminal, il choisit, en vue de satisfaire à la garantie d'authentification requise, plusieurs fournisseurs IdSP dans un groupe de fournisseurs IdSP qui ont des relations de confiance avec l'utilisateur, et demande à chacun des fournisseurs IdSP choisis d'authentifier l'utilisateur. Si tous les résultats d'authentification reçus des fournisseurs IdSP indiquent que l'utilisateur a été authentifié correctement, le fournisseur de services fournit son service au terminal.

Ce modèle permet de fournir une authentification multiple ou une authentification multiméthode. Il convient de noter que la méthode d'authentification employée dépend du groupe de fournisseurs IdSP.

Ce modèle permet aussi de fournir une authentification à facteur unique si la méthode d'authentification fournie par un fournisseur IdSP permet de satisfaire à la garantie d'authentification requise. Toutefois, l'authentification à facteur unique dans ce modèle sort du cadre de la présente Recommandation.

7.1.12 Modèle T-12

Dans le modèle T-12, plusieurs fournisseurs IdSP fournissent des méthodes d'authentification combinée, qui sont de types différents mais emploient le même facteur (c'est-à-dire des méthodes d'authentification multiple ou multiméthode), et plusieurs fournisseurs IdSP, un fournisseur de services et plusieurs terminaux sont connectés entre eux par l'intermédiaire du réseau. Et en particulier, dans ce modèle, un ou plusieurs utilisateurs n'ont pas de relation de confiance avec tous les fournisseurs IdSP.

NOTE – Il se peut que, dans ce modèle, un fournisseur IdSP n'ait de relation de confiance avec aucun des utilisateurs. Ce cas de figure sort toutefois du cadre de la présente Recommandation.

Lorsque le fournisseur de services reçoit une demande de service émanant du terminal, il choisit, en vue de satisfaire à la garantie d'authentification requise, un ou plusieurs fournisseurs IdSP dans un groupe de fournisseurs IdSP qui ont des relations de confiance avec l'utilisateur, et demande à chacun des fournisseurs IdSP choisis d'authentifier l'utilisateur. Si tous les résultats d'authentification reçus du ou des fournisseurs IdSP indiquent que l'utilisateur a été authentifié correctement, le fournisseur de services fournit son service au terminal.

Ce modèle permet de fournir une authentification multiple ou une authentification multiméthode, bien qu'il dépende du choix et du groupe des fournisseurs IdSP.

7.1.13 Modèle T-13

Dans le modèle T-13, plusieurs fournisseurs IdSP fournissent des méthodes d'authentification unique, qui emploient différents facteurs, et plusieurs fournisseurs IdSP, un fournisseur de services et plusieurs terminaux sont connectés entre eux par l'intermédiaire du réseau. Et en particulier, dans ce modèle, un ou plusieurs utilisateurs n'ont pas de relation de confiance avec tous les fournisseurs IdSP.

NOTE – Il se peut que, dans ce modèle, un fournisseur IdSP n'ait de relation de confiance avec aucun des utilisateurs. Ce cas de figure sort toutefois du cadre de la présente Recommandation.

Lorsque le fournisseur de services reçoit une demande de service émanant du terminal, il choisit, en vue de satisfaire à la garantie d'authentification requise, plusieurs fournisseurs IdSP dans un groupe de fournisseurs IdSP qui ont des relations de confiance avec l'utilisateur, et demande à chacun des fournisseurs IdSP choisis d'authentifier l'utilisateur. Si tous les résultats d'authentification reçus des fournisseurs IdSP indiquent que l'utilisateur a été authentifié correctement, le fournisseur de services fournit son service au terminal.

Ce modèle permet de fournir tous les types d'authentifications multiples. Il convient de noter que la méthode d'authentification employée dépend du choix des fournisseurs IdSP.

Ce modèle permet aussi de fournir une authentification à facteur unique si la méthode d'authentification fournie par un fournisseur IdSP permet de satisfaire à la garantie d'authentification requise. Toutefois, l'authentification à facteur unique dans ce modèle sort du cadre de la présente Recommandation.

7.1.14 Modèle T-14

Dans le modèle T-14, plusieurs fournisseurs IdSP fournissent des méthodes d'authentification combinée, qui emploient différents facteurs, et plusieurs fournisseurs IdSP, un fournisseur de services et plusieurs terminaux sont connectés entre eux par l'intermédiaire du réseau. Et en particulier, dans ce modèle, un ou plusieurs utilisateurs n'ont pas de relation de confiance avec tous les fournisseurs IdSP.

NOTE – Il se peut que, dans ce modèle, un fournisseur IdSP n'ait de relation de confiance avec aucun des utilisateurs. Ce cas de figure sort toutefois du cadre de la présente Recommandation.

Lorsque le fournisseur de services reçoit une demande de service émanant du terminal, il choisit, en vue de satisfaire à la garantie d'authentification requise, un ou plusieurs fournisseurs IdSP dans un groupe de fournisseurs IdSP qui ont des relations de confiance avec l'utilisateur, et demande à chacun des fournisseurs IdSP choisis d'authentifier l'utilisateur. Si tous les résultats d'authentification reçus du ou des fournisseurs IdSP indiquent que l'utilisateur a été authentifié correctement, le fournisseur de services fournit son service au terminal.

Ce modèle permet de fournir tous les types de méthodes d'authentification combinée.

7.2 Modèle de cycle de vie de l'authentification des entités

Le modèle de cycle de vie de l'authentification des entités est le modèle de transition d'états au cours de la phase d'authentification des entités qui est définie dans la référence [UIT-T X.1254].

Il y a deux types de modèles: le modèle de cycle de vie du point de vue de l'utilisateur et le modèle de cycle de vie du point du vue du fournisseur de services.

7.2.1 Modèle de cycle de vie du point de vue de l'utilisateur

Au cours de la procédure d'authentification du modèle de cycle de vie du point de vue de l'utilisateur, l'état d'authentification peut être l'un des suivants: "pas d'authentification", "identifié", "contrôlé" et "déconnecté" (Figure 2).

L'état d'authentification initial est "pas d'authentification".

Lorsque l'utilisateur envoie une demande d'authentification et est identifié par le fournisseur IdSP, l'état passe de "pas d'authentification" à "identifié".

Dès lors que l'utilisateur a été authentifié par le fournisseur IdSP, l'état passe de "identifié" à "contrôlé".

En outre, si l'utilisateur envoie une demande de déconnexion ou si un certain temps s'est écoulé depuis que l'utilisateur a été authentifié et que l'état est devenu "contrôlé", celui-ci passe de "contrôlé" à "déconnecté".

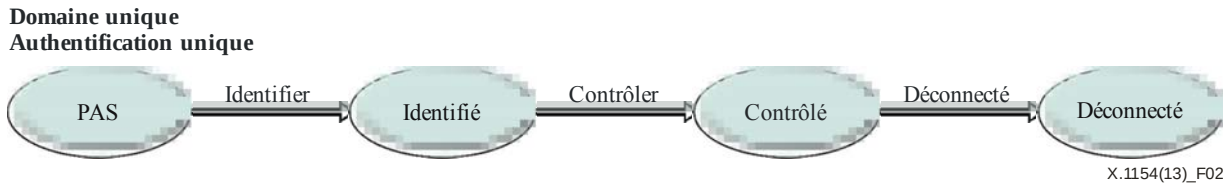

Figure 2 – Transition d'états lors de l'authentification à facteur unique

Dans le cas de l'authentification combinée, la transition d'états de "identifié" à "contrôlé" est différente (Figure 3).

Au cours de la procédure d'authentification combinée, le fournisseur IdSP ou le fournisseur de services gère la garantie d'authentification en vigueur de l'utilisateur.

Lorsque l'utilisateur est authentifié correctement à l'aide d'une authentification à facteur unique, la garantie d'authentification en vigueur est mise à jour et il est examiné si elle satisfait à la garantie d'authentification requise.

Si la garantie d'authentification en vigueur satisfait à la garantie d'authentification requise, l'état passe de "identifié" à "contrôlé".

En outre, si l'utilisateur envoie une demande de déconnexion ou si un certain temps s'est écoulé depuis que l'utilisateur a été authentifié et que l'état est devenu "contrôlé", celui passe de "contrôlé" à "déconnecté".

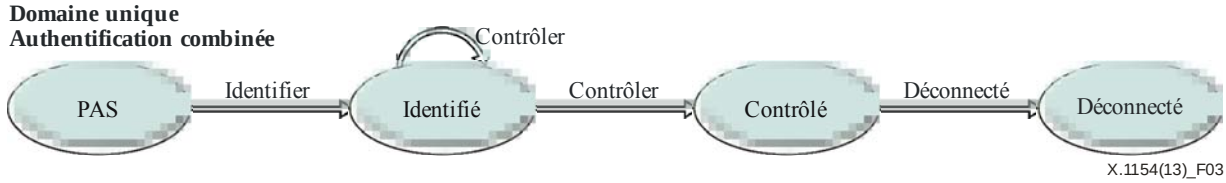

Figure 3 – Transition d'états lors de l'authentification combinée dans un domaine unique

La transition d'états représentée dans la Figure 4 concerne le cas d'une authentification combinée dans plusieurs domaines qui ont des exigences différentes en matière de garantie d'authentification selon les modèles T-4, T-6 et T-8.

Bien que la transition d'états dans le premier domaine soit la même que dans la Figure 3, celle dans les autres domaines est différente.

Lorsque l'état dans le premier domaine est "contrôlé pour le 1er domaine" et que l'utilisateur envoie une demande d'authentification au deuxième domaine, l'état dans le deuxième domaine passe à "insuffisant pour le 2ème domaine" si l'utilisateur est identifié dans le deuxième domaine. Si la garantie d'authentification en vigueur de l'utilisateur satisfait à la garantie d'authentification requise dans le deuxième domaine, l'état passe de "insuffisant pour le 2ème domaine" à "contrôlé pour le 2ème domaine".

Sinon, l'utilisateur est authentifié par le fournisseur IdSP (ou le fournisseur de services) et la garantie d'authentification en vigueur est mise à jour et il est examiné si elle satisfait à la garantie d'authentification requise. En outre, si l'utilisateur envoie une demande de déconnexion à un domaine quelconque, l'état dans tous les domaines passe de "contrôlé" à "déconnecté".

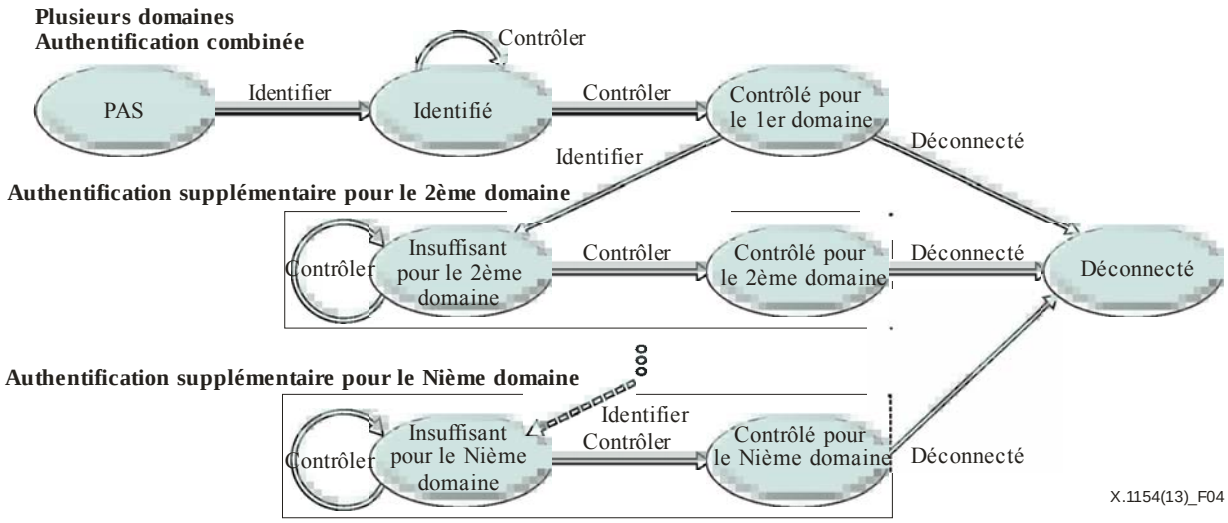

Figure 4 – Transition d'états lors de l'authentification combinée dans plusieurs domaines ayant des exigences différentes en matière de garantie d'authentification

La transition d'états représentée dans la Figure 5 concerne le cas d'une authentification combinée dans plusieurs domaines en fédération. Ce cas est identique à celui d'une authentification combinée dans plusieurs domaines qui ont des exigences différentes en matière de garantie d'authentification selon les modèles T-4, T-6 et T-8.

La transition d'états dans le premier domaine est la même que dans les Figures 3 et 4.

Lorsque l'état dans le premier domaine est "contrôlé" et que l'utilisateur envoie une demande d'authentification au deuxième domaine, l'état ne change pas, mais l'utilisateur est identifié dans le deuxième domaine.

En outre, si l'utilisateur envoie une demande de déconnexion à un domaine quelconque, l'état dans tous les domaines passe de "contrôlé" à "déconnecté".

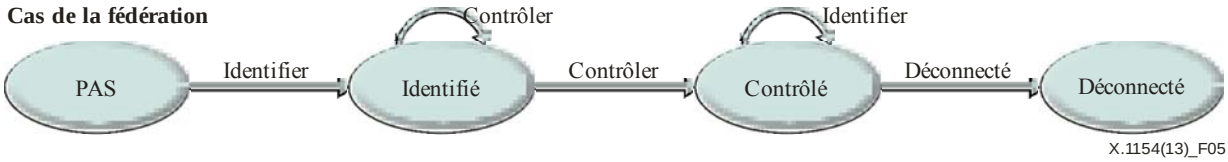

Figure 5 – Transition d'états lors de l'authentification combinée dans plusieurs domaines en fédération

7.2.2 Modèle de cycle de vie du point de vue du fournisseur de services

Au cours de la procédure d'authentification du modèle de cycle de vie du point de vue du fournisseur de services, l'état d'authentification peut être l'un des suivants: "pas d'authentification", "identifié", "contrôlé" et "déconnecté" (Figure 6).

L'état d'authentification initial est "pas d'authentification".

Lorsque le fournisseur de services reçoit une demande d'authentification et identifie l'utilisateur, l'état passe de "pas d'authentification" à "identifié". Après cette étape, l'état passe de "identifié" à "contrôlé" si l'utilisateur est authentifié par le fournisseur IdSP.

En outre, si le fournisseur de services reçoit une demande de déconnexion émanant de l'utilisateur ou si un certain temps s'est écoulé depuis que l'utilisateur a été authentifié et que l'état est devenu "contrôlé", celui passe de "contrôlé" à "déconnecté".

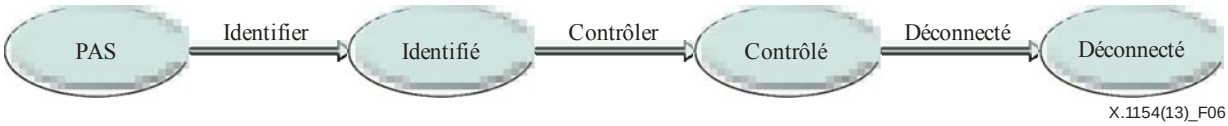

Figure 6 – Transition d'états lors de l'authentification à facteur unique

Dans le cas de l'authentification combinée, la transition d'états de "identifié" à "contrôlé" est différente.

Au cours de la procédure d'authentification combinée, le fournisseur IdSP ou le fournisseur de services gère la garantie d'authentification en vigueur de l'utilisateur.

Lorsque l'utilisateur est authentifié correctement par le fournisseur IdSP, la garantie d'authentification en vigueur est mise à jour et il est examiné si elle satisfait à la garantie d'authentification requise.

Si la garantie d'authentification en vigueur satisfait à la garantie d'authentification requise, l'état passe de "identifié" à "contrôlé".

En outre, si l'utilisateur envoie une demande de déconnexion ou si un certain temps s'est écoulé depuis que l'utilisateur a été authentifié et que l'état est devenu "contrôlé", celui passe de "contrôlé" à "déconnecté".

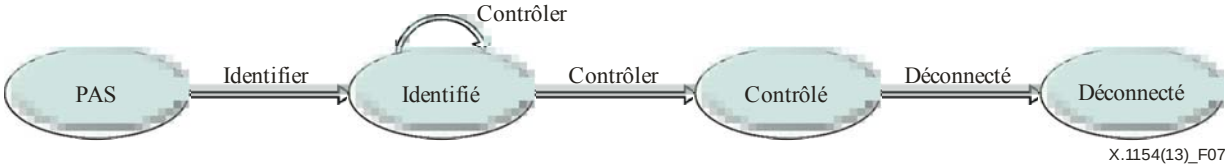

Figure 7 – Transition d'états lors de l'authentification combinée

Du point de vue du fournisseur de services, il n'y aucune différence par rapport à l'authentification combinée même si l'utilisateur accède à plusieurs domaines ou à des domaines fédérés.

8 Opérations dans des environnements à plusieurs fournisseurs de service d'identité

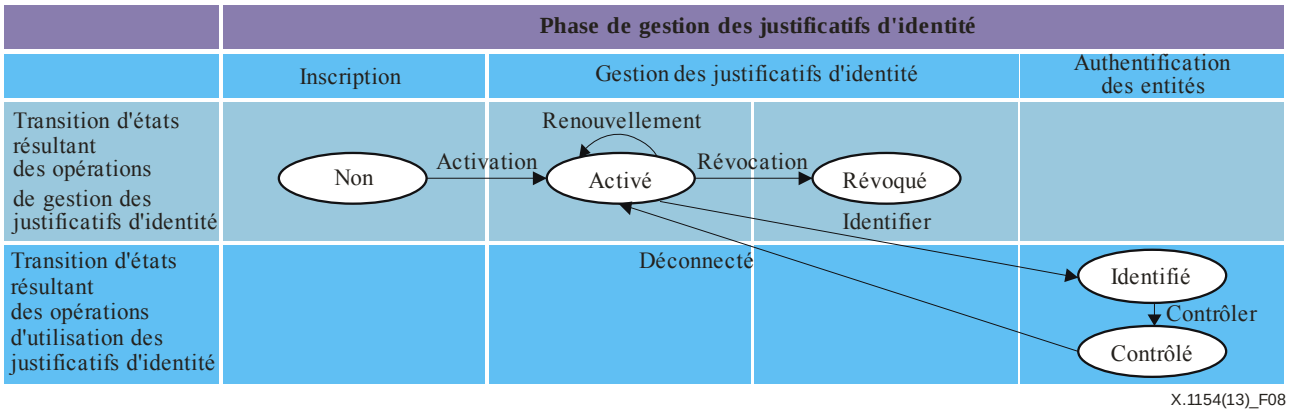

Figure 8 – Opérations effectuées par l'utilisateur

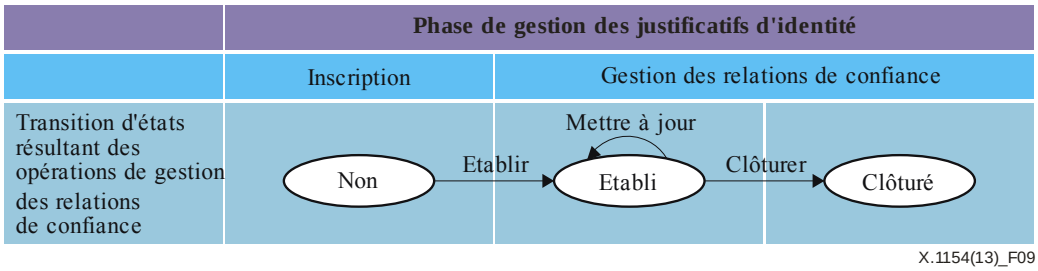

Figure 9 – Opérations effectuées par le fournisseur de services

Dans les modèles mentionnés au paragraphe 7, les types suivants d'opérations effectuées par le fournisseur IdSP sont décrits:

1) les opérations de gestion des justificatifs d'identité (Figure 8);
2) les opérations d'utilisation des justificatifs d'identité (Figure 8);
3) les opérations de gestion des relations de confiance avec les fournisseurs de services (Figure 9).

8.1 Opérations de gestion des justificatifs d'identité

Les opérations de gestion des justificatifs d'identité sont des opérations qui permettent à l'utilisateur de gérer comme suit la durée de vie de ses justificatifs d'identité:

1) Activation

   L'opération d'activation consiste à exécuter la procédure d'activation des justificatifs d'identité, qui est définie dans la référence [UIT-T X.1254], en vue de spécifier le justificatif d'identité de l'utilisateur.

2) Renouvellement

   L'opération de renouvellement consiste à exécuter la procédure de renouvellement des justificatifs d'identité, qui est définie dans la référence [UIT-T X.1254], en vue de spécifier le justificatif d'identité de l'utilisateur.

3) Révocation

   L'opération de révocation consiste à exécuter la procédure de révocation des justificatifs d'identité, qui est définie dans la référence [UIT-T X.1254], en vue de spécifier le justificatif d'identité de l'utilisateur.

8.2 Opérations d'utilisation des justificatifs d'identité

Si le justificatif d'identité est activé, les opérations d'utilisation peuvent être effectuées. Les opérations d'utilisation des justificatifs d'identité sont des opérations qui permettent l'identification/le contrôle de l'utilisateur et l'expiration de l'assertion qui a été délivrée au départ par l'opération de contrôle de l'utilisateur.

1) Identification

   L'opération d'identification permet d'identifier l'utilisateur.

   Cette opération est employée au cours de la phase d'authentification de l'entité.

2) Contrôle

   L'opération de contrôle permet de contrôler si l'entité homologue de communication est l'utilisateur déclaré dans le justificatif d'identité présenté. Dès lors que l'entité homologue de communication est contrôlée, une assertion est délivrée à l'entité homologue de communication.

   Cette opération est employée au cours de la phase d'authentification de l'entité.

3) Déconnexion

L'assertion expire après l'opération de déconnexion.

Cette opération est employée au cours de la phase d'utilisation.

8.3 Opérations de gestion des relations de confiance avec les fournisseurs de services

Les opérations de gestion des relations de confiance avec les fournisseurs de services sont des opérations qui permettent aux fournisseurs de services d'établir et de rompre les relations de confiance avec des fournisseurs de services.

1) Etablissement

L'opération d'établissement crée une nouvelle relation de confiance avec un certain fournisseur de services.

Cette opération est employée au cours de la phase d'inscription des relations de confiance.

2) Mise à jour

L'opération de mise à jour renouvelle la relation de confiance existante avec un certain fournisseur de services.

Cette opération est employée au cours de la phase de gestion des relations de confiance.

3) Clôture

L'opération de clôture détruit la relation de confiance spécifiée avec un fournisseur de services particulier.

Cette opération est employée au cours de la phase de gestion des relations de confiance.

9 Cadre général de l'authentification combinée dans des environnements à plusieurs fournisseurs de service d'identité

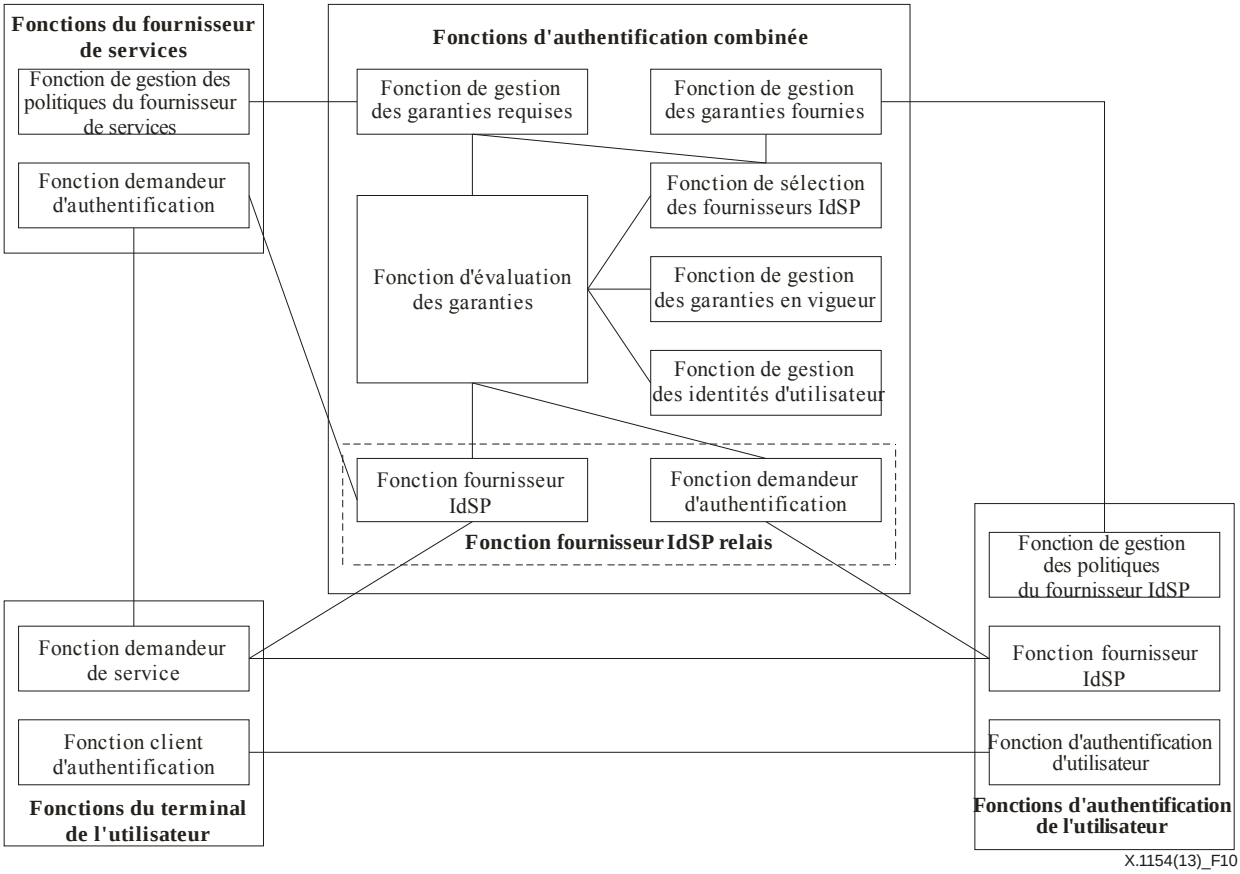

Figure 10 – Modèle pour le cadre général de l'authentification combinée dans des environnements à plusieurs fournisseurs de service d'identité

Dans la Figure 10, le cadre de l'authentification combinée contient quatre blocs de fonctions logiques: les fonctions d'authentification de l'utilisateur, les fonctions du fournisseur de services, les fonctions du terminal de l'utilisateur et les fonctions d'authentification combinée.

9.1 Composantes logiques

9.1.1 Fonctions d'authentification de l'utilisateur

Les fonctions d'authentification de l'utilisateur comportent trois fonctions: la fonction d'authentification d'utilisateur, la fonction fournisseur IdSP et la fonction de gestion des politiques du fournisseur IdSP.

La fonction d'authentification d'utilisateur est une fonction qui effectue l'opération de contrôle et authentifie un utilisateur.

La fonction fournisseur IdSP est une fonction qui reçoit une demande d'authentification émanant (d'une fonction demandeur d'authentification) des fonctions d'authentification combinée et effectue l'opération d'identification. En outre, la fonction fournisseur IdSP reçoit la demande de déconnexion et effectue l'opération de déconnexion.

La fonction de gestion des politiques du fournisseur IdSP est une fonction qui gère la politique d'authentification du fournisseur IdSP, comprenant un type de méthode d'authentification et un niveau de garantie d'authentification, fourni par la fonction d'authentification d'utilisateur.

9.1.2 Fonctions du fournisseur de services

Les fonctions du fournisseur de services comportent deux fonctions: la fonction demandeur d'authentification et la fonction de gestion des politiques du fournisseur de services.

La fonction demandeur d'authentification est une fonction qui envoie une demande d'authentification aux (à la fonction fournisseur IdSP des) fonctions d'authentification combinée.

La fonction de gestion des politiques du fournisseur de services est une fonction qui gère la politique d'authentification du fournisseur de services, comprenant un niveau de garantie d'authentification, exigé pour la fourniture d'un service.

9.1.3 Fonctions du terminal de l'utilisateur

Les fonctions du terminal de l'utilisateur comportent deux fonctions: la fonction demandeur de service et la fonction client d'authentification.

La fonction demandeur de service est une fonction qui envoie une demande de service aux (à une fonction demandeur d'authentification des) fonctions de fournisseur de services.

La fonction client d'authentification est une fonction qui communique avec (une fonction d'authentification d'utilisateur d') une fonction d'authentification à facteur unique pour authentifier l'utilisateur.

9.1.4 Fonctions d'authentification combinée

Les fonctions d'authentification combinée comportent huit fonctions: la fonction fournisseur IdSP, la fonction demandeur d'authentification, la fonction de gestion des garanties requises, la fonction de gestion des garanties fournies, la fonction de gestion des garanties en vigueur, la fonction de gestion des identités d'utilisateur, la fonction d'évaluation des garanties et la fonction de sélection des fournisseurs IdSP.

La fonction fournisseur IdSP est une fonction qui reçoit une demande d'authentification émanant (d'une fonction demandeur d'authentification) des fonctions de fournisseur de services et effectue l'opération d'identification. En outre, la fonction fournisseur IdSP reçoit la demande de déconnexion d'un service et effectue l'opération de déconnexion.

La fonction demandeur d'authentification est une fonction qui envoie une demande d'authentification ou une demande de déconnexion aux (à la fonction fournisseur IdSP des) fonctions d'authentification à facteur unique.

La fonction de gestion des garanties requises est une fonction qui gère le niveau de garantie d'authentification, exigé par chacune des fonctions de fournisseur de services, au moyen d'opérations d'établissement, de mise à jour et de terminaison.

La fonction de gestion des garanties fournies est une fonction qui gère le type de méthode et le niveau de garantie d'authentification, fourni par chacune des fonctions d'authentification à facteur unique, au moyen d'opérations d'établissement, de mise à jour et de terminaison.

La fonction de gestion des garanties en vigueur est une fonction qui gère le niveau de garantie d'authentification en vigueur de chacun des utilisateurs.

La fonction de gestion des identités d'utilisateur est une fonction qui gère les informations concernant les identités de chacun des utilisateurs, par l'intermédiaire des fonctions de création/de mise à jour/de révocation.

La fonction d'évaluation des garanties est une fonction qui contrôle le résultat de l'authentification de l'utilisateur fournie par la fonction fournisseur IdSP dans les fonctions d'authentification à facteur unique. C'est aussi une fonction qui évalue le niveau de garantie en vigueur de l'utilisateur et vérifie si celui-ci satisfait au niveau de garantie requis du fournisseur de services.

La fonction de sélection des fournisseurs IdSP est une fonction qui choisit une ou plusieurs fonctions d'authentification à facteur unique pour l'utilisateur, en vue de satisfaire au niveau de garantie requis du fournisseur de services.

Il convient de noter que certains cadres de gestion d'identités (IdM) existants peuvent employer une autre fonction, la fonction fournisseur relais de service d'identité, au lieu de la fonction fournisseur IdSP et de la fonction demandeur d'authentification.

9.2 Fonctionnements

9.2.1 Demande de service

La Figure 11 représente le fonctionnement générique d'une demande de service dans le cadre général de l'authentification combinée dans des environnements à plusieurs fournisseurs de service d'identité.

(1) Une fonction demandeur de service envoie une demande de service à la fonction demandeur d'authentification dans les fonctions du fournisseur de services.

(2) Lorsque la fonction demandeur d'authentification dans les fonctions du fournisseur de services reçoit la demande de service, elle envoie une demande d'authentification à la fonction fournisseur IdSP dans les fonctions d'authentification combinée, si elle juge que la fonction du terminal de l'utilisateur doit être authentifiée avant de fournir le service d'application.

(3) Lorsque la fonction fournisseur IdSP reçoit la demande de service, elle envoie la demande d'authentification à la fonction d'évaluation des garanties.

(4) La fonction d'évaluation des garanties récupère auprès de la fonction de gestion des garanties en vigueur le niveau de garantie en vigueur du terminal de l'utilisateur et envoie à une fonction de sélection des fournisseurs IdSP une demande de sélection des fournisseurs IdSP, accompagnée de la garantie en vigueur du terminal de l'utilisateur.

(5) La fonction de sélection des fournisseurs IdSP récupère auprès de la fonction de gestion des garanties requises et de la fonction de gestion des garanties fournies, le niveau de garantie requise du fournisseur de services et le niveau de garantie fournie pour chacun des fournisseurs IdSP. Puis, elle choisit, dans une liste des fournisseurs IdSP disponibles, un fournisseur IdSP et envoie son nom à la fonction d'évaluation des garanties.

(6) La fonction d'évaluation des garanties récupère, si nécessaire, auprès de la fonction de gestion des identités d'utilisateur l'identificateur du terminal de l'utilisateur pour le fournisseur IdSP choisi, et envoie une demande d'authentification à la fonction demandeur d'authentification. Puis, la fonction demandeur d'authentification envoie une demande d'authentification à la fonction fournisseur IdSP dans les fonctions du fournisseur IdSP choisi.

(7) La fonction fournisseur IdSP envoie la demande d'authentification à la fonction d'authentification. Puis, la fonction d'authentification authentifie l'utilisateur à l'aide de la fonction client d'authentification dans les fonctions du terminal de l'utilisateur.

(8) La fonction d'authentification renvoie les résultats d'authentification à la fonction d'évaluation des garanties, par l'intermédiaire de la fonction fournisseur IdSP dans les fonctions du fournisseur IdSP et de la fonction demandeur d'authentification dans les fonctions d'authentification combinée.

(9) La fonction d'évaluation des garanties évalue et met à jour la garantie en vigueur du terminal de l'utilisateur.

(10) Si le niveau de garantie en vigueur du terminal de l'utilisateur n'est pas suffisant pour la fourniture du service (c'est-à-dire s'il est inférieur à la garantie requise), la fonction d'évaluation des garanties effectue à nouveau, auprès de la fonction de sélection des fournisseurs IdSP, une demande de sélection des fournisseurs IdSP. Puis, les étapes 5) à 9) sont reproduites.

(11) Si le niveau de garantie en vigueur du terminal de l'utilisateur est suffisant pour fournir le service au cours de l'étape 10), la fonction d'évaluation des garanties envoie un résultat d'authentification à la fonction fournisseur IdSP.

(12) La fonction fournisseur IdSP crée une assertion et l'envoie à la fonction demandeur d'authentification dans les fonctions du fournisseur de services.

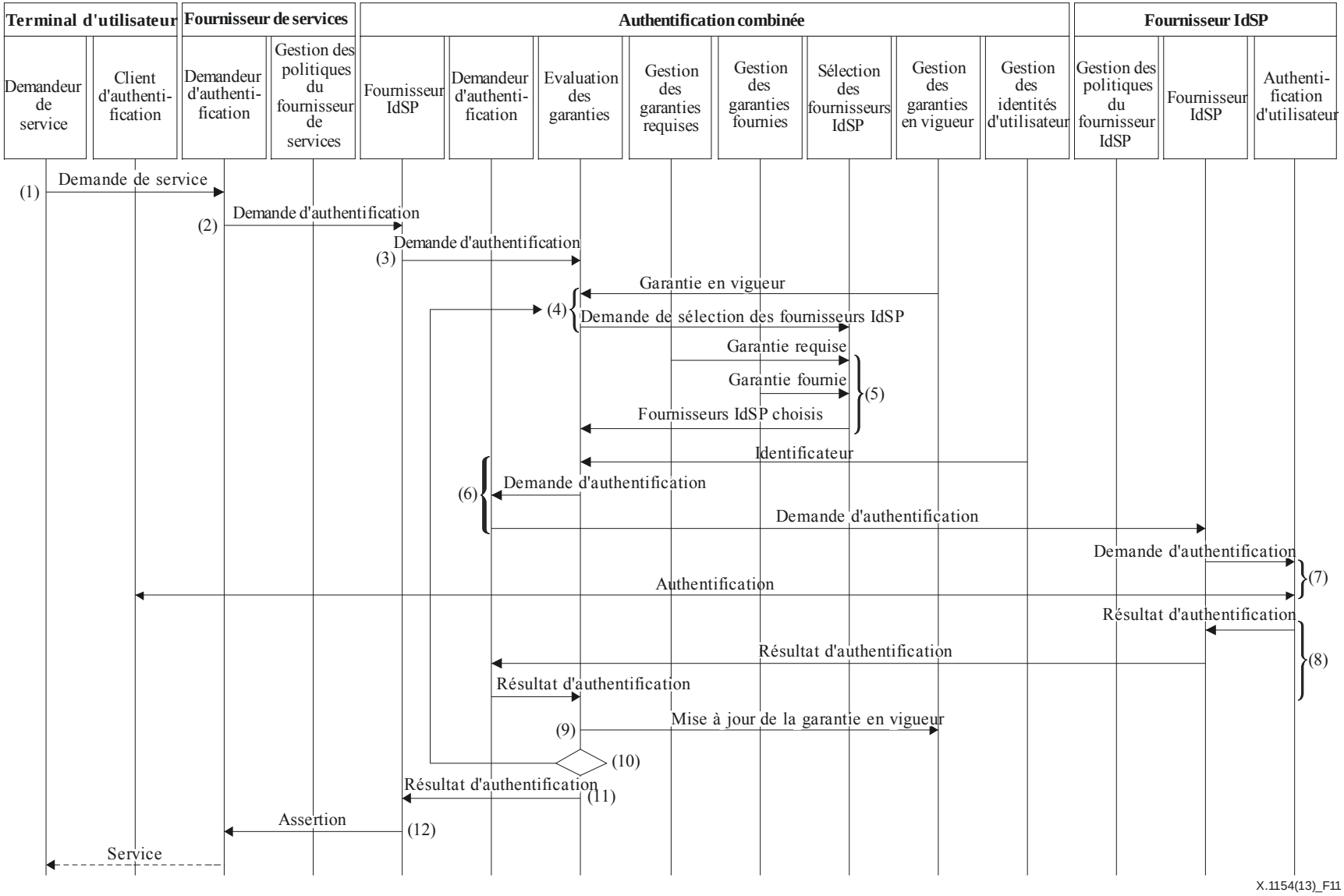

Figure 11 – Fonctionnement générique d'une demande de service dans le cadre général de l'authentification combinée dans des environnements à plusieurs fournisseurs de service d'identité

9.2.2 Clôture de service

La Figure 12 représente le fonctionnement générique d'une clôture de service dans le cadre général de l'authentification combinée dans des environnements à plusieurs fournisseurs de service d'identité.

1) Une fonction demandeur de service envoie une demande de clôture de service à la fonction demandeur d'authentification dans les fonctions du fournisseur de services.
2) Lorsque la fonction demandeur d'authentification dans les fonctions du fournisseur de services reçoit la demande de clôture de service, elle envoie une demande de déconnexion à la fonction fournisseur IdSP dans les fonctions d'authentification combinée.
3) Lorsque la fonction fournisseur IdSP reçoit la demande de déconnexion, elle envoie la demande de clôture à la fonction d'évaluation des garanties.
4) La fonction d'évaluation des garanties récupère une liste des fournisseurs IdSP auxquels le terminal de l'utilisateur est connecté et envoie une demande de déconnexion à toutes les fonctions fournisseur IdSP énumérées, par l'intermédiaire de la fonction demandeur d'authentification.
5) La fonction fournisseur IdSP renvoie un résultat de déconnexion.
6) Lorsque la fonction d'évaluation des garanties reçoit les résultats de déconnexion, la garantie en vigueur est mise à jour.
7) Lorsque la fonction d'évaluation des garanties a reçu l'ensemble des résultats de déconnexion, elle renvoie un résultat de clôture à la fonction fournisseur IdSP.
8) La fonction fournisseur IdSP renvoie le résultat de déconnexion à la fonction demandeur d'authentification.
9) La fonction demandeur d'authentification renvoie le résultat de clôture de service à la fonction demandeur de service.

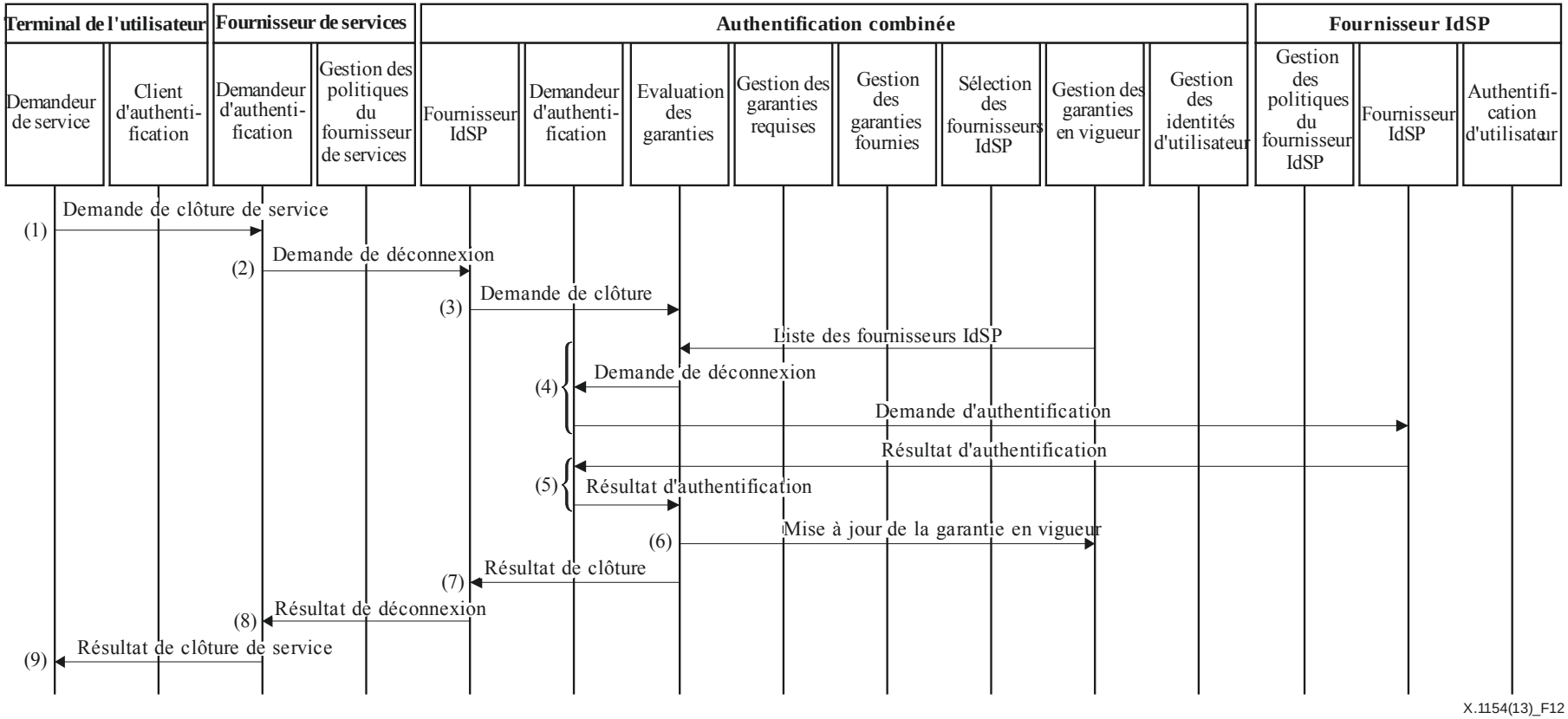

Figure 12 – Fonctionnement générique d'une clôture de service dans le cadre général de l'authentification combinée dans des environnements à plusieurs fournisseurs de service d'identité

9.2.3 Gestion des garanties requises des fonctions fournisseur de services

En vue de la gestion des garanties requises des fonctions fournisseur de services dans les fonctions d'authentification combinée, une garantie requise est envoyée par la fonction de gestion des politiques du fournisseur de services à la fonction de gestion des garanties requises, au moyen des opérations établir/mettre à jour/clôturer.

9.2.4 Gestion des garanties fournies des fonctions fournisseur IdSP

En vue de la gestion des garanties fournies des fonctions fournisseur de services dans les fonctions d'authentification combinée, une garantie requise est envoyée par la fonction de gestion des politiques du fournisseur IdSP à la fonction de gestion des garanties fournies, au moyen des opérations établir/mettre à jour/clôturer.

Annexe A

Considérations relatives à l'authentification combinée

(Cette annexe fait partie intégrante de la présente Recommandation.)

A.1 Obtention d'une garantie d'authentification donnée

Puisque l'authentification combinée est une authentification qui emploie plusieurs justificatifs d'identité, des justificatifs d'identité différents doivent être utilisés pour obtenir une garantie d'authentification donnée. Autrement dit, la simple association de plusieurs méthodes d'authentification ou de plusieurs fournisseurs IdSP conduira à un échec total du niveau de garantie si le même justificatif d'identité est employé.

Pour obtenir une garantie d'authentification donnée, il faut disposer d'une procédure permettant de contrôler si les justificatifs d'identité employés dans l'authentification combinée sont différents ou non. Il est recommandé d'exécuter cette procédure de contrôle avant la mise à jour de la garantie d'authentification en vigueur.

Dans le modèle où une fonction d'authentification combinée et des fonctions d'authentification d'utilisateur sont intégrées dans la même entité (par exemple, un fournisseur IdSP fournit une authentification combinée), il est facile d'exécuter la procédure de contrôle au niveau du fournisseur IdSP. En outre, la procédure de contrôle pourrait être exécutée lorsque l'opération de création/mise à jour est effectuée.

Par ailleurs, dans le modèle où une fonction d'authentification combinée et des fonctions d'authentification d'utilisateur sont intégrées dans la même entité (par exemple, le fournisseur de services emploie plusieurs fournisseurs IdSP fournissant une authentification à facteur unique), un échange de données supplémentaire entre la fonction d'authentification combinée et la fonction d'authentification d'utilisateur est nécessaire dans le cadre de la procédure de contrôle. En particulier, il est nécessaire d'intégrer dans la fonction d'authentification d'utilisateur une fonction qui envoie des données permettant d'identifier le justificatif d'identité. En outre, il est nécessaire d'intégrer dans la fonction d'authentification combinée une fonction qui confirme, en comparant chacune des données reçues des fonctions d'authentification d'utilisateur, qu'un justificatif d'identité différent est employé.

Dans le cas où la méthode d'authentification employée repose sur l'infrastructure de clé publique (PKI), la fonction dans la fonction d'authentification de l'utilisateur peut envoyer une clé publique en tant qu'information contenant le justificatif d'identité, et la fonction dans la fonction d'authentification combinée peut vérifier cette information directement.

Toutefois, dans le cas où la méthode d'authentification employée fait appel à un secret partagé (par exemple, un mot de passe), il est interdit à la fonction dans la fonction d'authentification de l'utilisateur d'envoyer le secret partagé lui-même en tant qu'information contenant le justificatif d'identité.

A.2 Sélection du ou des fournisseurs de service d'identité

Lorsque le fournisseur de services reçoit une demande de service émanant du terminal, il est impératif que la fonction de sélection des fournisseurs IdSP découvre et choisisse le ou les fournisseurs IdSP appropriés.

En vue de procéder à la sélection du fournisseur IdSP approprié, il faut que la fonction de gestion des garanties requises et que la fonction de gestion des garanties fournies soient assurées de manière sécurisée.

Par ailleurs, la fonction de gestion des garanties en vigueur doit être assurée de manière sécurisée au niveau du fournisseur IdSP (dans le modèle où un seul fournisseur IdSP fournit une fonction d'authentification combinée) ou du fournisseur de services (dans le modèle où le fournisseur de services fournit la fonction d'authentification combinée).

En outre, la fonction d'évaluation des garanties doit récupérer de manière sécurisée la garantie d'authentification en vigueur, la garantie d'authentification requise et la garantie d'authentification fournie.

A.3 Garantie d'authentification réelle

Dans certains cas, la garantie d'authentification réelle peut être moindre que la garantie d'authentification prévue, les changements étant dus à divers facteurs environnementaux.

Dans ces cas, une fonction devant envoyer la garantie d'authentification réelle au fournisseur de services doit être présente au niveau du fournisseur IdSP. En outre, une fonction doit être présente au niveau du fournisseur de services afin de mettre à jour et d'évaluer la garantie d'authentification en vigueur de l'utilisateur en se fondant sur la garantie d'authentification réelle.

A.4 Considérations relatives à la sécurité pour l'authentification multifacteur

Il y a deux types d'authentifications multifacteurs: celui où un justificatif d'identité unique est employé pour le contrôle et celui où plusieurs justificatifs d'identité sont employés pour le contrôle.

Le premier type d'authentification repose sur un certificat de clé publique enregistré sur une carte à puce ou sur un mot de passe à usage unique, qui utilise un équipement matériel.

Le second type d'authentification repose sur l'association d'un mot de passe à usage unique et de facteurs biométriques.

Le premier type d'authentification multifacteur doit employer du matériel inviolable pour l'enregistrement des justificatifs d'identité.

A.5 Considérations relatives à la sécurité pour l'authentification multiméthode

Dans le cas d'authentification multiples, il est impératif que chacun des justificatifs d'identité ne puisse pas être déduit (ou deviné) à partir d'autres justificatifs d'identité.

A.6 Considérations relatives à la sécurité pour l'authentification multiple

Dans le cas de plusieurs authentifications, il est impératif que chacun des justificatifs d'identité ne puisse pas être déduit (ou deviné) à partir d'autres justificatifs d'identité.

Appendice I

Relations avec des normes similaires

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

I.1 Relation avec la référence [UIT-T X.1141]

La Figure I.1 illustre la relation entre le modèle décrit dans la présente Recommandation et celui qui est décrit, dans le langage de balisage d'assertion de sécurité (SAML 2.0), au paragraphe 10 de la référence [UIT-T X.1141]. Les cadres grisés sont des fonctions définies dans le langage SAML.

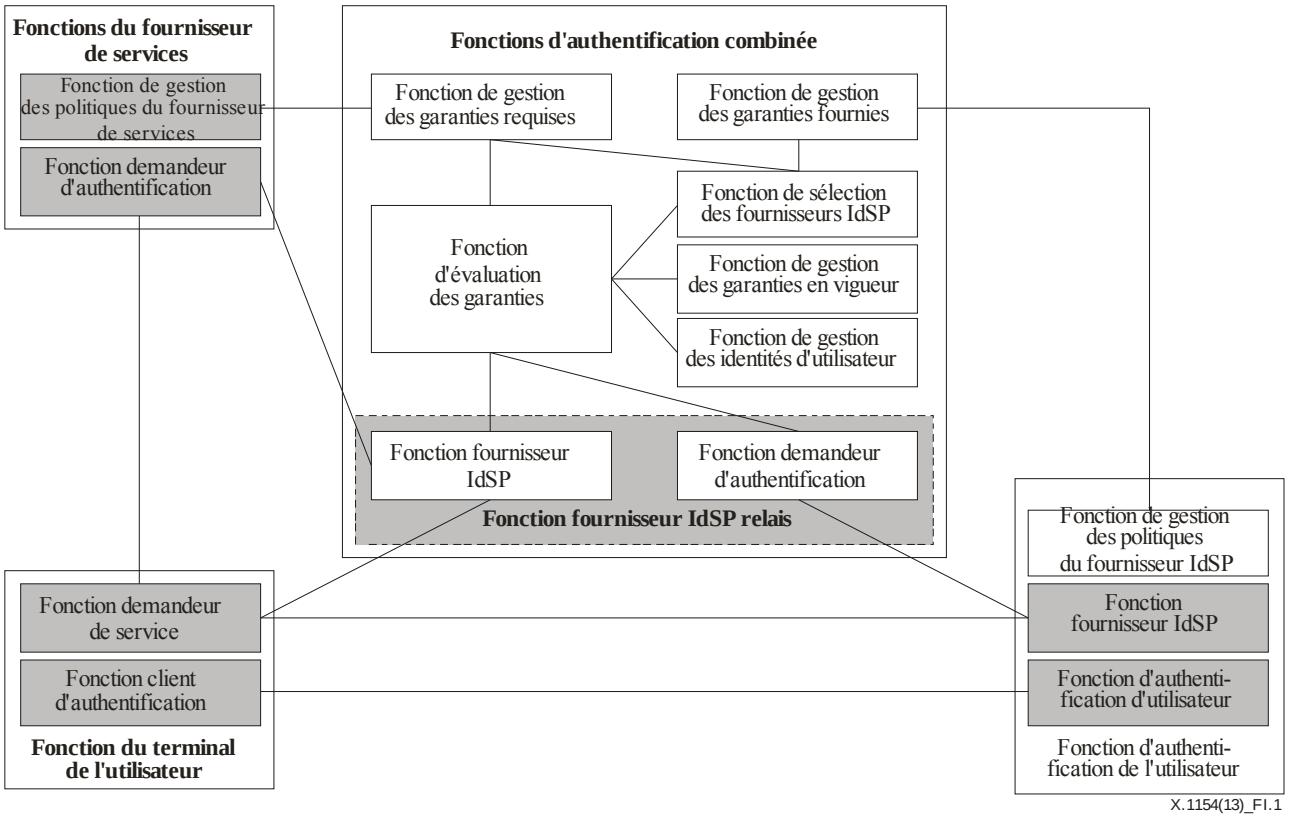

Figure I.1 – Relation avec la référence [UIT-T X.1141]

I.2 Relation avec la référence [UIT-T X.1254]

Le cadre de la présente Recommandation permet d'effectuer une authentification combinée en employant plusieurs fournisseurs IdSP. Cela signifie que ce cadre est l'une des manières de réaliser, dans des environnements à plusieurs fournisseurs IdSP, la phase d'authentification qui est décrite dans la référence [UIT-T X.1254].

Bibliographie

[b-UIT-T X.509] Recommandation UIT-T X.509 (2008) | ISO/CEI 9594-8:2008, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

[b-UIT-T X.1084] Recommandation UIT-T X.1084 (2008), *Mécanisme de système télébiométrique – Partie 1*: *Protocole général d'authentification biométrique et profils types pour les systèmes de télécommunication*.

[b-UIT-T X.1086] Recommandation UIT-T X.1086 (2008), *Procédures de protection télébiométriques – Partie 1: Lignes directrices relatives aux mesures techniques et de gestion pour la sécurité des données biométriques*.

[b-UIT-T X.1089] Recommandation UIT-T X.1089 (2008), *Infrastructure d'authentification télébiométrique*.

[b-UIT-T X.1151] Recommandation UIT-T X.1151 (2007), *Lignes directrices applicables à un protocole d'authentification sûre fondée sur un mot de passe avec échange de clés*.

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

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, 2013