Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1254

(09/2020)

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

Sécurité du cyberespace – Gestion des identités

Cadre de garantie d'authentification des entités

Recommandation UIT-T X.1254

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 (1)	
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 (1)	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 spam	X.1230–X.1249
Gestion des identités	**X.1250–X.1279**
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
SÉCURITÉ DE LA 5G	X.1800–X.1819

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

Recommandation UIT-T X.1254

Cadre de garantie d'authentification des entités

Résumé

La Recommandation UIT-T X.1254 définit trois niveaux de garantie d'authentification (AAL) des entités ainsi que les critères et menaces correspondant à chacun de ces trois niveaux.

En outre:

- elle spécifie un cadre de gestion des niveaux AAL;
- elle fournit, d'après une évaluation des risques, des orientations concernant les techniques de contrôle à utiliser pour réduire les menaces sur l'authentification;
- elle donne des orientations relatives à l'application des trois niveaux AAL à d'autres systèmes de garantie d'authentification; et
- elle donne des orientations quant à l'échange des résultats d'authentification reposant sur les trois niveaux AAL.

Historique

Édition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1254	07-09-2012	17	11.1002/1000/11608
2.0	UIT-T X.1254	03-09-2020	17	11.1002/1000/14260

Mots clés

AAL, garantie, authentification, niveau de garantie d'authentification, gestion d'identité, IdM, niveau de garantie, LoA.

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

AVANT-PROPOS

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

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

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

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

NOTE

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

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on 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

Une identité numérique est la représentation unique d'une entité engagée dans une transaction en ligne. La garantie – ou la confiance dans le fait – que l'identité numérique avec laquelle il y a interaction correspond à l'identité déclarée est au cœur de la confiance, de la sécurité et du contrôle d'accès. On identifie trois types de garantie qui contribuent à instaurer la confiance dans une identité numérique: la garantie d'identité, la garantie d'authentification et la garantie de fédération.

La présente Recommandation fournit un cadre de garantie d'authentification. Aux fins de la présente Recommandation, l'authentification est définie comme la procédure de vérification d'une identité déclarée pour la réalisation d'une transaction en ligne. Dans le cadre de services nécessitant des visites répétées, l'authentification permet de garantir, sur une base de risque raisonnable, que l'utilisateur qui accède au service aujourd'hui est le même que celui qui a accédé au service précédemment.

Le cadre défini dans la présente Recommandation permet aux fournisseurs de services en ligne – parties utilisatrices et fournisseurs de services de justificatifs d'identité (CSP) – de disposer d'une approche systématique permettant de comprendre les risques encourus et d'identifier les contrôles utilisés pour les atténuer. Il vise à faciliter la sélection méthodique des contrôles et des stratégies d'atténuation des risques selon un processus en trois étapes:

1) identification des rôles et des services pour définir les catégories de menaces;
2) mise en place d'un processus de gestion des risques ciblé pour déterminer la puissance des contrôles requis; et
3) identification des technologies – protocoles, types de justificatifs d'identité, etc. – utilisées pour affiner davantage les contrôles.

Un modèle basé sur les menaces

La présente Recommandation vise à faciliter la sélection méthodique des contrôles et des stratégies d'atténuation des risques. Une étape préliminaire, pour pouvoir sélectionner les contrôles et stratégies d'atténuation appropriés, consiste à identifier les types de risques et de menaces associés au(x) rôle(s) et services d'un prestataire de services en ligne. Voir la Figure 0-1.

Figure 0-1 – Services, risques et contrôles

Le cadre est structuré sur la base de catégories de risques et de menaces, qui fournissent aux prestataires de services en ligne un lien fonctionnel entre les processus d'évaluation des risques d'une part et les activités de contrôle et d'atténuation des risques d'autre part.

Les prestataires de services d'identité peuvent fournir tout ou partie des composants fonctionnels de ces phases d'identité numérique, ou même un seul de ces composants. À ce titre, il convient d'évaluer les risques et de se pencher sur les contrôles et stratégies d'atténuation de ces risques sur la base d'une approche multicomposantes similaire à celle utilisée pour le cycle de vie des transactions numériques. La présente Recommandation traite des risques et des contrôles associés aux phases de gestion des justificatifs et d'authentification de ce cycle de vie. D'autres documents (par exemple, [b-ISO/CEI TS 29003]) abordent les risques et les contrôles pour les activités liées à l'inscription et à la vérification d'identité ainsi que les contrôles organisationnels et de gestion. Ces documents ainsi que d'autres devraient être alignés de manière à obtenir un ensemble coordonné de normes sur la gestion des identités (comme illustré dans la Figure 0-2) qui, lorsqu'elles sont associées, définissent les processus, les risques et les contrôles relatifs au cycle de vie des transactions sur les identités numériques.

On trouvera en outre dans la présente Recommandation une liste de menaces pesant sur la vie privée, de considérations et de contrôles d'atténuation entrant dans son champ d'application (authentification et gestion des justificatifs d'identité). La présente Recommandation ne tient pas compte des considérations liées à la vie privée en ce qui concerne les inscriptions et les vérifications d'identité.

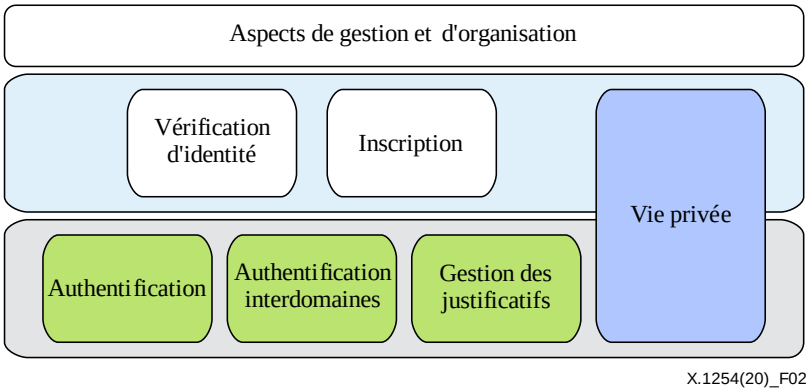

Figure 0-2 – Normes alignées fondamentales sur la gestion des identités

Lien avec la version précédente de la présente Recommandation

La première édition de la présente Recommandation [b-UIT-T X.1254 (2012)] présentait le cycle de vie des transactions numériques au travers de trois phases: l'inscription et la vérification d'identité; la gestion des justificatifs d'identité; et l'authentification des identités. Le secteur a évolué depuis 2012 et de nouveaux concepts et approches ont vu le jour tels que l'authentification sans mot de passe et l'authentification renforcée. Le secteur, qui reposait sur un concept de niveau de garantie (LoA), utilise désormais une seule échelle ordinale qui définit les exigences spécifiques à la mise en œuvre. En combinant la gestion appropriée des risques liés aux activités économiques et à la protection de la vie privée avec les besoins de la mission, les responsables de la mise en œuvre sélectionneront des niveaux de garantie d'identité (IAL), des niveaux de garantie d'authentification (AAL) et des niveaux de garantie de fédération (FAL) comme options distinctes. La présente Recommandation traite des niveaux AAL. Les niveaux IAL et FAL ne relèvent pas de son champ d'application.

Recommandation UIT-T X.1254

Cadre de garantie d'authentification des entités

1 Domaine d'application

La présente Recommandation fournit un cadre permettant de gérer la garantie d'authentification des entités (EAA) dans un contexte donné. En particulier:

– elle définit trois niveaux de garantie d'authentification (AAL) des entités;

– elle fournit des orientations pour comprendre ces niveaux;

– elle définit des critères et des lignes directrices permettant d'atteindre les niveaux spécifiés pour la garantie EAA;

– elle donne des orientations relatives à la comparaison et au mappage entre les mécanismes de garantie d'authentification;

– elle donne des orientations quant à l'échange des résultats d'authentification, fondés sur des niveaux de garantie spécifiques; et

– elle donne des orientations concernant les contrôles qui devraient être utilisés pour atténuer les menaces pour l'authentification sur la base d'une évaluation des risques.

2 Références

Aucune.

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 sa validité.

NOTE – Il est généralement admis que les termes assertion et déclaration sont très semblables, leurs significations différant néanmoins légèrement. Aux fins de la présente Recommandation, une assertion est considérée comme étant une affirmation plus forte qu'une déclaration.

3.1.2 authentification [b-ISO/CEI 18014-2]: attestation de l'identité déclarée par une entité.

3.1.3 facteur d'authentification [b-ISO/CEI 19790]: information et/ou procédure employées pour authentifier ou contrôler l'identité d'une entité.

NOTE – Les facteurs d'authentification appartiennent à l'une des quatre catégories suivantes:

– une chose que possède l'entité (par exemple, signature de dispositif, passeport, dispositif matériel contenant un justificatif d'identité, clé privée);

– une chose que connaît l'entité (par exemple, mot de passe, numéro d'identification personnel (PIN));

– une chose qu'est l'entité (par exemple, ses caractéristiques biométriques); ou

– une chose que fait généralement l'entité (par exemple, son attitude comportementale).

3.1.4 protocole d'authentification [b-ISO/CEI 29115]: séquence définie de messages entre une entité et un contrôleur, qui permet à celui-ci d'authentifier l'entité.

3.1.5 déclaration [b-UIT-T X.1252]: affirmation selon laquelle une chose est vraie, même si la preuve ne peut être fournie.

NOTE – Il est généralement admis que les termes assertion et déclaration sont très semblables, leurs significations différant néanmoins légèrement. Aux fins de la présente Recommandation, une assertion est considérée comme étant une affirmation plus forte qu'une déclaration.

3.1.6 contexte [b-UIT-T X.1252]: environnement aux limites définies dans lequel les entités existent et interagissent.

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

NOTE – Voir l'Appendice I pour des caractéristiques supplémentaires d'un justificatif d'identité.

3.1.8 entité [b-UIT-T X.1252]: une chose ayant une existence séparée et distincte, qui peut être identifiée dans un contexte.

NOTE – Aux fins de la présente Recommandation, l'entité est aussi employée dans le cas particulier d'une chose qui déclare une identité.

3.1.9 identité, identité partielle [b-ISO/CEI 24760-1]: ensemble d'attributs se rapportant à une identité.

NOTE – Dans un contexte particulier, une identité peut avoir un ou plusieurs identificateurs pour permettre à une entité d'être reconnue de façon unique dans ce contexte.

3.1.10 contrôle des informations d'identité [b-ISO/CEI 29115]: procédure de vérification, s'agissant de l'authenticité, de la validité, de l'exactitude et du lien avec l'entité, des informations et des justificatifs d'identité auprès des émetteurs, des sources de données ou d'autres ressources internes ou externes.

3.1.11 vérification d'identité [b-ISO/CEI 29115]: procédure au moyen de laquelle l'autorité d'enregistrement recueille et contrôle un nombre suffisant d'informations pour identifier une entité à un niveau de garantie spécifié ou convenu.

3.1.12 attaque de l'intercepteur [b-ISO/CEI 29115]: attaque dans laquelle l'auteur est capable de lire, d'insérer ou de modifier des messages entre deux parties, à leur insu.

3.1.13 authentification multifacteur [b-ISO/CEI 19790]: authentification au moyen de deux facteurs indépendants d'authentification au moins.

3.1.14 authentification mutuelle [b-ISO/CEI 29115]: authentification des identités d'entités, qui donne à chacune des deux entités une garantie quant à l'identité de l'autre.

3.1.15 non-répudiation [b-UIT-T X.1252]: capacité de protection contre le fait que l'une des entités impliquées dans une action nie avoir participé à tout ou partie de l'action.

3.1.16 hameçonnage [b-ISO/CEI 29115]: escroquerie au moyen de laquelle le destinataire d'un message électronique est frauduleusement amené à révéler des informations personnelles ou confidentielles que l'escroc peut ensuite utiliser à des fins illicites.

3.1.17 répudiation [b-UIT-T X.1252]: fait que l'une des entités impliquées nie avoir participé à tout ou partie d'une action.

3.1.18 évaluation des risques [b-ISO/CEI 27000]: ensemble du processus d'identification du risque, d'analyse du risque et d'évaluation du risque.

3.1.19 secret partagé [b-ISO/CEI 29115]: secret employé dans l'authentification, qui n'est connu que par l'entité et le contrôleur.

3.1.20 transaction [b-ISO/CEI 29115]: événement discret faisant intervenir une entité et un fournisseur de services et ayant lieu à des fins commerciales ou à des fins de programmation.

3.1.21 vérification [b-ISO/CEI 29115]: procédure de confrontation des informations fournies avec des informations précédemment corroborées.

3.1.22 contrôleur [b-ISO/CEI 29115]: acteur corroborant des informations relatives à l'identité.

NOTE – Le contrôleur peut intervenir au cours de plusieurs phases du cadre de garantie d'authentification des entités et vérifier les justificatifs d'identité et/ou les informations d'identité.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 fournisseur de services de justificatifs d'identité *(*CSP*, credential service provider)*: acteur de confiance délivrant ou gérant des justificatifs d'identité.

NOTE – Cette définition est fondée sur celle figurant dans [b-ISO/CEI 29115].

3.2.2 garantie d'authentification d'entité *(*EAA*, entity anthentication assurance)*: degré de confiance atteint au cours de la procédure d'authentification, selon lequel l'entité est ce qu'elle est ou ce qu'elle devrait être.

NOTE 1 – La confiance est fondée sur le degré de confiance dans le lien entre l'entité et l'identité présentée.

NOTE 2 – Cette définition est fondée sur celle de la garantie d'authentification figurant dans [b-UIT-T X.1252].

3.2.3 identificateur: un ou plusieurs attributs caractérisant de façon unique une entité dans un contexte particulier.

NOTE – Cette définition est fondée sur celle figurant dans [b-UIT-T X.1252].

3.2.4 autorité d'enregistrement (RA, *registration authority*): acteur de confiance qui établit ou se porte garant de l'identité d'une entité auprès d'un fournisseur de services de justificatifs d'identité (CSP).

NOTE – Cette définition est fondée sur celle figurant dans [b-ISO/CEI 29115].

3.2.5 partie utilisatrice (RP, *relying party*): acteur se fiant à une assertion ou à une déclaration d'identité.

NOTE – Cette définition est fondée sur celle figurant dans [b-ISO/CEI 29115].

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AAL niveau de garantie d'authentification (*authentification assurance level*)

CSP fournisseur de services de justificatifs d'identité (*credential service provider)*

EAA garantie d'authentification des entités (*entity authentification assurance)*

FAL niveau de garantie de fédération (*federation assurance level)*

FIDO authentification rapide en ligne (*fast identity on-line*)

HTML langage de balisage hypertexte (*hypertext markup language*)

HTTP protocole de transfert hypertexte (*hypertext transfer protocol*)

HTTPS protocole de transfert hypertexte sécurisé (*hypertext transfer protocol-secure*)

IAL niveau de garantie d'identité (*identity assurance level*)

IdM gestion d'identité (*identity management*)

IDP fournisseur d'identité (*identity provider*)

LoA niveau de garantie (*level of assurance*)

MAC commande d'accès au support (*media access control*)

MITM homme du milieu, intercepteur (*man in the middle*)

MITB homme dans le navigateur (*man in the browser*)

OAuth authentification ouverte (*open authentication*)

OpenID identité ouverte (*open identity*)

OTP mot de passe à usage unique (*one time password*)

PIA évaluation des incidences sur la vie privée (*privacy impact assessment*)

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

PIN numéro d'identification personnel (*personal identification number*)

RA autorité d'enregistrement (*registration authority*)

RP partie utilisatrice (*relying party*)

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

TLS sécurité de couche de transport (*transport layer security*)

URL identificateur uniforme de ressources (*uniform resource locator*)

5 Conventions

La présente Recommandation emploie les formes des verbes ci-après lors de la formulation des dispositions.

a) "doit" désigne une obligation.

b) "devrait" désigne une recommandation.

c) "pourra" désigne une permission.

d) "peut" désigne une possibilité ou une capacité.

6 Flux de processus d'authentification numérique

6.1 Généralités

L'identité numérique désigne la représentation unique d'une entité engagée dans une transaction en ligne. Dans sa forme la plus simple, l'authentification numérique consiste à vérifier, dans une certaine mesure, l'identité déclarée d'une entité afin de lui donner accès à un service en ligne. Une entité enregistrée tente de s'authentifier auprès d'un service en ligne en faisant apparaître la possession d'un authentificateur, également connu sous le nom de justificatif d'identité, délivré au moment de l'enregistrement. Le service en ligne – également appelé partie utilisatrice dans la transaction – tente ensuite de vérifier la validité de l'authentificateur auprès du fournisseur d'identité (IDP) ou du fournisseur de services de justificatifs d'identité (CSP) ou du contrôleur. L'entité peut accéder au service en ligne après contrôle de son justificatif d'identité par le fournisseur CSP/contrôleur.

La Figure 6-1 présente le flux de processus d'authentification numérique suivant:

1) une entité accède au service en ligne d'une partie utilisatrice;

2) la partie utilisatrice redirige l'entité vers le fournisseur CSP pour authentification;

3) le fournisseur CSP vérifie que l'entité est bien en possession de l'authentificateur ou des authentificateurs enregistré(s);

4) le fournisseur CSP envoie une assertion d'authentification à la partie utilisatrice pour affirmer le statut d'authentification de l'entité; et

5) une session authentifiée est établie entre l'entité et la partie utilisatrice.

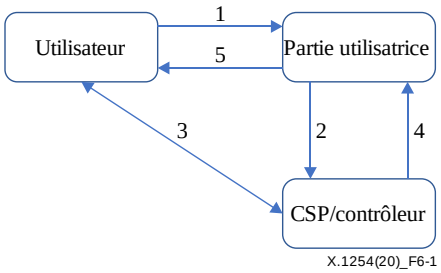

Figure 6-1 – Flux de processus d'authentification numérique

Le fait de présenter le flux de processus d'authentification numérique de cette façon fournit une méthode permettant de comprendre les risques associés aux divers rôles et fonctions impliqués dans l'authentification numérique.

Bien que la partie utilisatrice possède sa propre solution de gestion d'identité (IdM) et agisse comme son propre fournisseur CSP, cette Recommandation mentionne la partie utilisatrice et le fournisseur CSP comme deux rôles distincts. Cependant, dans un cas comme dans l'autre, les fonctions sont les mêmes.

De plus, la Figure 6-1 regroupe les rôles du fournisseur CSP et du contrôleur. Même si les fournisseurs de services de justificatifs exécutent généralement la fonction de vérification, un fournisseur CSP peut, dans certains cas, faire appel à un contrôleur distinct.

Le processus d'authentification numérique décrit ci-avant suppose que les entités sont déjà inscrites auprès d'un fournisseur CSP et détiennent un ou plusieurs authentificateurs enregistrés. Les procédures d'inscription et d'enregistrement ne relèvent pas du domaine d'application de la présente Recommandation.

6.2 Garantie d'identité numérique

Il est nécessaire de comprendre comment les services qui portent sur les phases et les composantes fonctionnelles du cycle de vie de l'identité numérique interagissent pour renforcer la confiance globale dans les transactions en ligne. Ce niveau de confiance est généralement exprimé sous la forme de degrés ou niveaux de garantie. La présente Recommandation contient des prescriptions et donne des orientations concernant la phase de garantie d'authentification des identités numériques et les fonctions de composantes du cadre global régissant l'identité numérique et la garantie d'authentification. La Figure 6-2 présente les composantes, la description de la garantie et les activités opérationnelles pour un ensemble de documents IdM de base alignés pour assurer la garantie et les contrôles dans le cadre global des identités numériques.

Composante de garantie	Descriptions	Activités
IA *Garantie d'identité*	Solidité du processus de vérification d'identité et du lien entre l'authentificateur et l'individu dont l'identité a été vérifiée.	• Vérification d'identité • Résolution • Validation • Vérification • Inscription • Association
AA *Garantie d'authentification*	Confiance dans le fait qu'un déclarant donné est le même que l'abonné qui a été précédemment authentifié.	• Authentification • Gestion des justificatifs • Délivrance des justificatifs • Suspension, révocation et/ou destruction des justificatifs • Renouvellement et/ou remplacement des justificatifs
FA *Garantie de fédération*	Combine les aspects du modèle de fédération, la force de la protection de l'assertion et la présentation de l'assertion.	• Gestion de clés • Décisions d'exécution • Gestion d'attributs

X.1254(20)_F6-2

Figure 6-2 – Niveaux de garantie d'identité numérique

Garantie d'identité: cette garantie est fondée sur des processus mis en place pour vérifier l'association d'un sujet avec son identité réelle. La garantie d'identité est traitée dans [b-ISO/CEI TS 29003].

Garantie d'authentification: l'authentification établit qu'un sujet tentant d'accéder à un service numérique contrôle les technologies utilisées pour s'authentifier. Cette garantie est fondée sur des processus permettant de vérifier qu'une identité déclarée est bien la même que celle qui a participé au processus d'enregistrement et qui a déjà été authentifiée par le système.

Garantie de fédération: cette garantie est fondée sur un ou des processus permettant de communiquer, de protéger et de valider les assertions d'identité fournies dans différents domaines de sécurité. La fédération d'identité concerne le partage d'informations d'identité et d'authentification en ligne entre deux parties ou plus.

Les composantes et activités de garantie d'identité pour la garantie de fédération n'entrent pas dans le cadre de cette édition de la présente Recommandation.

6.3 Rôles

6.3.1 Généralités

A l'instar d'un modèle centré sur les risques, le flux de processus d'authentification numérique aide à identifier les catégories de menaces associées à trois rôles principaux: fournisseurs CSP, parties utilisatrices et entités.

6.3.2 Fournisseurs de services en ligne

Les fournisseurs de services en ligne sont des organisations qui offrent des services, des applications et des informations en ligne nécessitant un accès restreint, tels que les services bancaires, les services de prestataires de soins de santé et les détaillants. Selon la façon dont le service est mis en œuvre, les fournisseurs de services en ligne peuvent jouer un ou plusieurs des rôles suivants:

- fournisseur CSP;
- fournisseur de services d'identité;
- contrôleur;

- partie utilisatrice.

6.3.3 Fournisseur de services de justificatifs d'identité

Les fournisseurs CSP sont chargés de contrôler le justificatif d'identité (par exemple, un authentificateur) présenté par l'entité. La procédure et le degré de rigueur avec lesquels ils le font sont déterminés par le niveau de risque associé à la transaction en ligne et à l'environnement dans lequel l'identité sera utilisée. La fonction CSP peut être exécutée depuis un système IdM d'un fournisseur de services en ligne en interne ou depuis un système de gestion d'identité d'une tierce partie. Qui plus est, le CSP est souvent responsable des activités de gestion des justificatifs.

6.3.4 Fournisseur de services d'identité

Les fournisseurs de services d'identité sont chargés de vérifier l'identité déclarée d'une entité et de garantir que l'identité déclarée est bien associée au justificatif fourni par l'entité. La procédure et le degré de rigueur avec lesquels ils le font sont déterminés par le niveau de risque associé à la transaction en ligne et à l'environnement dans lequel l'identité sera utilisée. Le fournisseur IDP peut être également responsable de l'enregistrement et de l'inscription des entités au sein de programmes et de services spécifiques. Les risques et les contrôles portant sur ces fonctions de composante IDP n'entrent pas dans le cadre de la présente Recommandation.

Le fournisseur IDP peut par ailleurs jouer le rôle de fournisseur CSP. Sachant que la présente Recommandation porte essentiellement sur l'authentification et la gestion des justificatifs d'identité, le terme de fournisseur CSP, lorsqu'il est utilisé, vise également à représenter un fournisseur IDP qui jouerait ce rôle dans une transaction.

6.3.5 Contrôleur

Les contrôleurs sont chargés de confirmer l'identité de l'entité en vérifiant la possession et le contrôle par l'entité d'un ou de plusieurs authentificateurs à l'aide d'un protocole d'authentification. Pour ce faire, le contrôleur peut également avoir besoin de valider les justificatifs d'identité qui lient le ou les authentificateurs à l'identificateur de l'entité et de vérifier leur statut. Le rôle du contrôleur est souvent joué par le CSP ou l'IDP qui fournit les services de justificatifs.

6.3.6 Partie utilisatrice

Les parties utilisatrices acceptent (s'appuient sur) et utilisent des assertions de statut d'authentification des entités émanant de leurs propres services IdM ou de fournisseurs CSP externes. Les parties utilisatrices doivent pouvoir avoir confiance dans les informations d'identité qu'elles reçoivent de ces services afin de prendre des décisions basées sur les risques pour autoriser ou non des entités spécifiques à accéder à leurs services et produits en ligne.

6.3.7 Entités

Aux fins de la présente Recommandation, les entités sont les utilisateurs des services offerts par les fournisseurs de services en ligne.

Les entités sont responsables de la protection de leurs identités et de leurs justificatifs numériques contre la fraude et l'utilisation abusive ainsi que de l'utilisation de leurs justificatifs selon les prescriptions convenues.

6.4 Composantes du processus d'authentification

La présente Recommandation fournit aux prestataires de services une méthodologie leur permettant d'identifier les menaces et les risques associés à leur service, en fonction de leur(s) rôle(s) – décrit(s) au paragraphe 6.3 – et des technologies de base.

Pour faciliter l'évaluation des risques et des menaces spécifiques associés à un service en ligne, il est important de savoir quelles sont les fonctions et les technologies d'appui qui sont impliquées dans le processus d'authentification.

Les composantes du processus sont les suivantes:

- les authentificateurs, par exemple les secrets mémorisés (tels que les mots de passe), les dispositifs à mot de passe à usage unique (OTP), les certificats numériques et paramètres biométriques (tels que les empreintes);
- les logiciels client et serveur;
- les protocoles de communication et d'authentification, par exemple HTML (langage de balisage hypertexte), SAML (langage de balisage d'assertion de sécurité), TLS (sécurité de la couche transport), Oauth (authentification ouverte) et OpenID (identité ouverte).

Les transactions d'authentification font l'objet d'attaques visant à compromettre les transactions, qui ciblent les vulnérabilités associées à une ou plusieurs des composantes listées dans l'alinéa précédent. La plupart des technologies d'authentification, incluant le matériel, les logiciels et les protocoles de communication, sont exposées à des menaces et vulnérabilités connexes spécifiques. Dans le cadre de leurs activités d'évaluation des risques, les fournisseurs de services en ligne doivent tenir compte des vulnérabilités associées à chaque composante. Le paragraphe 8 décrit les catégories de menaces, les risques et les contrôles spécifiques.

6.4.1 Authentificateurs

Un authentificateur est quelque chose qu'une entité possède et contrôle et qui est utilisé pour authentifier l'identité de l'entité. Plusieurs authentificateurs peuvent être associés à une entité. Les facteurs d'authentification incluent une chose que connaît l'entité, comme un mot de passe; une chose que possède l'entité, comme une carte à puce; et une chose qu'est l'entité, comme un paramètre biométrique. La rigueur d'une transaction d'authentification est renforcée par l'utilisation d'un ou de plusieurs facteurs différents.

Un fournisseur de services en ligne doit tenir compte du profil de risque de son service lorsqu'il sélectionne les authentificateurs acceptables pour l'authentification auprès de ce service. De plus, la partie utilisatrice doit tenir compte des exigences de garantie de son service avant d'accepter les services d'un fournisseur CSP.

Les types d'authentificateurs sont les suivants:

- secrets mémorisés;
- secrets de recherche;
- dispositifs hors bande;
- dispositifs OTP à un seul facteur;
- dispositifs OTP à plusieurs facteurs;
- logiciels cryptographiques à un seul facteur;
- dispositifs cryptographiques à un seul facteur;
- logiciels cryptographiques à plusieurs facteurs;
- dispositifs cryptographiques à plusieurs facteurs.

6.4.2 Authentificateur

Un objet ou une structure de données qui lie avec autorité une identité – via un ou des identificateurs – et (éventuellement) des attributs supplémentaires à au moins un authentificateur détenu et contrôlé par un abonné. Bien qu'il soit couramment admis que l'entité conserve l'authentificateur, la présente Recommandation utilise également le terme d'authentificateur pour faire référence aux enregistrements électroniques conservés par le fournisseur CSP, qui établissent un lien entre le ou les authentificateurs de l'abonné et son identité. La forme d'authentificateur la plus courante consiste en un nom d'utilisateur et des données d'utilisateur associées liés à un mot de passe ou à un autre authentificateur.

7 Utilisation de la gestion des risques dans le cadre de la garantie d'authentification

7.1 Généralités

Un système IdM, pour être efficace, dépend de la compréhension des niveaux de risques associés aux types de services en ligne offerts par l'organisation. Pour comprendre ces risques, les fournisseurs de services en ligne doivent tenir compte de leur(s) rôle(s) spécifique(s) au sein du cadre; de la nature de leurs utilisateurs; et des types de données et de transactions traitées par leurs applications.

L'application d'une méthode de gestion des risques structurée débouchera sur les résultats suivants: identification des risques et des menaces, décisions quant à la manière de les traiter et contributions nécessaires pour sélectionner et mettre en œuvre les contrôles. Dans le domaine de la gestion d'identité, des lignes directrices spécifiques existent pour aider les organisations à comprendre comment ces niveaux de risque correspondent aux niveaux de garantie, c'est-à-dire au degré relatif de confiance dans l'intégrité des identités en ligne.

Les fournisseurs de services en ligne doivent utiliser une méthode de gestion des risques et élaborer un plan de gestion des risques associés à l'authentification numérique.

La portée de l'évaluation des risques associés à l'identité numérique doit tenir compte, au minimum, du type et du niveau d'impact associés à chaque risque identifié. Il sera également tenu compte de la probabilité d'occurrence de chacun de ces risques.

7.2 Risques liés à l'authentification

Lorsque l'on considère les risques liés à l'authentification, la question fondamentale qui se pose est de savoir quelles seront les répercussions si l'authentification échoue, c'est-à-dire quel sera l'impact si l'accès est accordé à une entité qui n'est pas le propriétaire légitime du justificatif et du compte associé.

Lorsqu'ils évaluent leurs risques associés à l'échec d'authentification, les fournisseurs de services en ligne doivent tenir compte des éléments suivants:

- Données – L'identification des types de données traitées et protégées à l'intérieur des frontières du système est un élément clé permettant de déterminer ce qui est en jeu. Ces types de données incluent les informations d'identification personnelle (PII), les données financières, propriétaires, accessibles au public et hautement sensibles.
- Utilisateurs – L'identification et la compréhension des utilisateurs d'un système ou d'une entreprise sont fondamentales pour pouvoir identifier et classer les risques spécifiques. Les catégories d'utilisateurs sont les utilisateurs internes, externes et privilégiés. Les organisations devraient également déterminer si leurs utilisateurs sont liés par des accords contractuels, juridiques ou autres.
- Motifs de l'attaque – Si elle commence par définir ses utilisateurs et ses types de données, l'organisation sera davantage en mesure de comprendre les motifs des attaques. Par exemple, si le système traite et protège des informations bancaires, l'auteur d'une attaque peut être motivé par le gain financier pour accéder frauduleusement au système.

Les fournisseurs de services en ligne doivent choisir des contrôles et autres solutions d'atténuation des menaces sur la base d'une évaluation des risques.

8 Catégories de menaces, risques et contrôles

Ce paragraphe fournit une liste des risques et des contrôles, organisés par catégories de menaces. Les fournisseurs de services d'identité devraient identifier les catégories de menaces spécifiques auxquelles ils sont soumis, en fonction de leur(s) rôle(s) et service(s) liés à l'authentification. Les contrôles sont regroupés selon les catégories de menaces suivantes:

- compromission de l'authentificateur;

- compromission de la transaction;
- usurpation de l'identité du fournisseur CSP;
- usurpation de l'identité de l'entité;
- compromission du service d'authentification.

Les parties utilisatrices et les fournisseurs CSP partagent la responsabilité d'assurer la protection contre toutes les menaces d'authentification. Les rôles et les responsabilités impliqués dans une transaction d'authentification doivent être clairement établis et adoptés par toutes les parties.

Le Tableau 8-1 présente les catégories de menaces pesant sur l'authentification et les rôles généralement attribués pour atténuer ces menaces.

Tableau 8-1 – Rôles et catégories de menaces

Rôle	Catégories de menaces
Partie utilisatrice	• Usurpation de l'identité du contrôleur • Compromission de la transaction • Vie privée • Fédération
Fournisseur CSP	• Usurpation de l'identité du contrôleur • Compromission de la transaction • Usurpation de l'identité de l'abonné • Compromission de l'authentificateur • Compromission du service d'authentification • Vie privée • Fédération

8.1 Niveaux de garantie

Dans la présente Recommandation, l'authentification est le processus par lequel une identité déclarée est vérifiée dans le but de réaliser une transaction en ligne. Plus la rigueur apportée dans la procédure de vérification des identités déclarées sera grande, plus la confiance que l'identité authentifiée est bien le sujet prévu de cette identité sera présente. La garantie d'authentification est une mesure de cette confiance, et il existe des systèmes – ou schémas – qui définissent une série de niveaux de confiance relatifs, appelés niveaux AAL.

La présente Recommandation décrit un modèle de garantie d'authentification basé sur le concept d'identification et d'atténuation des menaces et des risques pour les transactions d'authentification. Dans de nombreux cas, les organisations, les organismes nationaux et les communautés d'intérêt peuvent choisir d'établir un schéma AAL qui regroupe les risques, les menaces et les contrôles liés aux environnements dans lesquels ils opèrent. Cette option présente de nombreux avantages tangibles, parmi lesquels la mise en place d'exigences pour la participation aux transactions à des niveaux communément définis et la possibilité de créer des packs de produits standard pour répondre aux besoins de la communauté.

La présente Recommandation délaisse le concept de niveau de garantie (LoA) en tant qu'ordinal unique régissant les exigences spécifiques à la mise en œuvre. À la place, en combinant la gestion appropriée des risques liés aux activités économiques et à la protection de la vie privée avec les besoins de la mission, les responsables de la mise en œuvre sélectionneront des niveaux IAL, AAL et FAL (niveau de garantie de fédération) comme options distinctes. Quand bien même de nombreux systèmes auraient le même niveau numérique pour chacun des niveaux IAL, AAL et FAL, ceci n'est pas une obligation et les responsables de la mise en œuvre ne doivent pas conclure qu'il en sera de même dans tous les systèmes.

Les composantes de la garantie d'identité décrites dans ces lignes directrices sont les suivantes:

- IAL correspond à la procédure de vérification d'identité;
- AAL correspond à la procédure d'authentification;
- FAL correspond à la force de l'assertion dans un environnement fédéré, utilisé pour communiquer des informations d'authentification et d'attribut (le cas échéant) à une partie utilisatrice.

Le fait de séparer ces catégories offre aux agents de mise en œuvre une flexibilité dans le choix des solutions d'identité et permet d'inclure plus facilement des techniques visant à renforcer la protection de la vie privée en tant qu'éléments fondamentaux des systèmes d'identité à tous les niveaux de garantie. Par exemple, ce modèle prend en charge des scénarios autorisant des interactions de pseudonymes même lorsque des authentificateurs puissants à plusieurs facteurs sont utilisés.

Dans le contexte actuel, les solutions d'identité mises à disposition des organisations se présentent sous une forme monolithique dans laquelle un système ou un vendeur fournit toutes les fonctionnalités. Un service d'identité peut comprendre plusieurs composantes qui permettent aux organisations et aux agences d'utiliser des solutions d'identité connectables et fondées sur les normes, en fonction des besoins de la mission.

Les trois niveaux AAL définissent les sous-ensembles d'options que les agents de mise en œuvre peuvent sélectionner en fonction de leur profil de risque et des dommages potentiels causés par l'auteur d'une attaque qui prendrait le contrôle d'un authentificateur et accéderait aux systèmes des agences. Ces niveaux sont les suivants:

Niveau de garantie d'authentification 1: Le niveau AAL1 fournit une certaine garantie que l'entité contrôle un authentificateur lié au compte de l'entité. Ce niveau requiert une authentification à un seul facteur ou à plusieurs facteurs utilisant une large gamme de technologies d'authentification disponibles. Pour s'authentifier avec succès, le déclarant doit prouver être en possession et contrôler l'authentificateur via un protocole d'authentification sécurisé.

Niveau de garantie d'authentification 2: Le niveau AAL2 garantit un niveau élevé de confiance dans le fait que l'entité contrôle le ou les authentificateurs liés au compte de l'entité. Les protocoles d'authentification nécessitent de démontrer être en possession ou contrôler deux facteurs d'authentification distincts. Des techniques cryptographiques mondialement acceptées sont requises pour les niveaux AAL2 et supérieurs.

Niveau de garantie d'authentification 3: Le niveau AAL3 garantit un niveau très élevé de confiance dans le fait que l'entité contrôle le ou les authentificateurs liés au compte de l'entité. L'authentification AAL3 est fondée sur la preuve de la possession d'une clé au moyen d'un protocole cryptographique. Elle utilise un authentificateur cryptographique basé sur le matériel et un authentificateur qui fournit une résistance à l'usurpation de l'identité du contrôleur; le même dispositif peut répondre à ces deux exigences. Pour s'authentifier au niveau AAL3, les déclarants doivent démontrer être en possession ou contrôler deux facteurs d'authentification distincts, via un ou plusieurs protocoles d'authentification sécurisés. Des techniques cryptographiques mondialement acceptées sont requises.

Cette édition de la présente Recommandation ne propose pas un ensemble unique de niveaux de garantie normatifs standard. Tenter de créer une structure de garantie unique standard pour toutes les communautés réduirait la capacité de certaines communautés à gérer les risques en fonction de leur environnement. Elle reconnaît cependant que ces différents schémas de garantie existent et que les fournisseurs de services d'identité doivent souvent être en mesure de démontrer leur adhésion à un ou plusieurs ensembles de niveaux AAL.

Étant donné que les schémas AAL montrent des niveaux de confiance croissants en ce qui concerne la vérification d'une identité déclarée, avec des niveaux de rigueur eux-aussi croissants au niveau de la procédure d'authentification, la présente Recommandation utilise des termes relatifs plutôt que des niveaux AAL discrets dans la description des contrôles. Aux fins de ces contrôles qui peuvent être

modifiés pour accroître la confiance, l'appellation "niveau AAL le plus bas" correspond à un moindre niveau de confiance, "niveau AAL supérieur" à un niveau de confiance supérieur et "niveau AAL le plus élevé" à un niveau de confiance encore supérieur. Le Tableau 8-2 donne une représentation théorique de la façon dont cette convention pourrait correspondre à certains des schémas de garantie d'authentification les plus courants. (Il est à noter que, dans le Tableau 8-2, l'alignement n'est en aucun cas destiné à établir une équivalence directe entre les différents schémas.)

Tableau 8-2 – Niveaux de garantie d'authentification

Niveau AAL	Schéma à quatre niveaux AAL	Schéma à trois niveaux AAL	Schéma à trois niveaux
Le plus élevé	Niveau AAL 4	Niveau AAL 3	Élevé
Supérieur	Niveau AAL 3	Niveau AAL 2	Important
	Niveau AAL 2		
Le plus bas	Niveau AAL 1	Niveau AAL 1	Bas

Le reste du présent paragraphe fournit un surensemble de contrôles normatifs, regroupés en fonction des menaces qu'ils atténuent. Les fournisseurs de services d'identité doivent identifier les menaces spécifiques auxquelles ils sont soumis en fonction de leurs rôles et services, comme décrit dans la présente Recommandation. Une fois que cela est déterminé, et afin d'être en mesure d'évaluer la conformité à la présente Recommandation, les fournisseurs de services d'identité doivent documenter les menaces de même que les descriptions de contrôle correspondantes et les résultats souhaités, comme prévu dans le reste de la présente clause.

8.2 Compromission de l'authentificateur

8.2.1 Risques de compromission de l'authentificateur

On entend par compromission de l'authentificateur toute attaque qui duplique, altère ou entraîne la divulgation non autorisée d'informations relatives aux justificatifs, qui peuvent être utilisées pour s'authentifier avec succès et obtenir un accès non autorisé à un système d'information. La compromission de l'authentificateur peut survenir à tout moment du cycle de vie IdM. Cependant, les menaces et les contrôles qui entrent dans le cadre de la présente Recommandation sont uniquement en lien avec l'authentification.

Les informations relatives aux justificatifs peuvent être compromises par un certain nombre de vecteurs d'attaque, notamment l'hameçonnage, le vol, la duplication des justificatifs, l'attaque par répétition et les attaques en force brute en ligne ou hors ligne. La protection contre le risque de compromission des justificatifs n'est pas l'apanage exclusif de cette catégorie de menaces. Il est à noter qu'une compromission des justificatifs peut être une conséquence des échecs de contrôle dans l'une ou l'autre des catégories de menaces. Par exemple, si un fournisseur de services d'authentification subit une violation de données, les informations obtenues peuvent être utilisées pour obtenir un accès non autorisé au système d'information.

8.2.2 Contrôles empêchant la compromission de l'authentificateur

Le Tableau 8-3 dresse la liste des contrôles visant à empêcher la compromission de l'authentificateur.

Tableau 8-3 – Contrôles empêchant la compromission de l'authentificateur

CTRL #	Description du contrôle	Résultat attendu
AC-1	Pour le niveau AAL le plus élevé, l'authentification devrait utiliser un authentificateur cryptographique basé sur le matériel et un authentificateur qui fournit une résistance à l'usurpation de l'identité du contrôleur – un même dispositif peut répondre à ces deux exigences.	Les authentificateurs appropriés sont utilisés pour atteindre le niveau AAL souhaité.
AC-2	Pour le niveau AAL le plus élevé, les déclarants devraient démontrer être en possession ou contrôler deux facteurs d'authentification distincts, via un ou plusieurs protocoles d'authentification sécurisés.	Les protocoles d'authentification appropriés sont appliqués pour atteindre le niveau AAL souhaité.
AC-3	Les authentificateurs à plusieurs facteurs utilisés au niveau AAL le plus élevé devraient être validés dans la mesure requise par un programme de vérification de module cryptographique approuvé.	La cryptographie de l'authentificateur est validée dans la mesure nécessaire pour atteindre le niveau AAL souhaité.
AC-4	Les authentificateurs obtenus par les fournisseurs IDP devraient être validés pour répondre aux exigences du programme de vérification de module cryptographique approuvé.	La cryptographie approuvée est utilisée.
AC-5	Le contrôleur devrait mettre en place des contrôles pour se protéger contre les attaques en ligne par devinette, si applicables au type d'authentificateur.	Le contrôleur met en place des contrôles pour protéger les authentificateurs contre les attaques en ligne par devinette.
AC-6	Sauf disposition contraire dans la description d'un authentificateur donné, le contrôleur devrait limiter à 100 le nombre de tentatives d'authentification infructueuses consécutives sur un même compte.	Le contrôleur met en place des contrôles pour protéger les authentificateurs contre les attaques en ligne par devinette.
AC-7	Les authentificateurs cryptographiques devraient utiliser la cryptographie approuvée.	La cryptographie approuvée est utilisée.
AC-8	Si plusieurs authentificateurs sont utilisés pour l'authentification, l'un deux au moins devrait être résistant à la répétition.	Les authentificateurs sont protégés contre les attaques par répétition.
AC-9	Tous les authentificateurs de dispositifs cryptographiques devraient être résistants à la répétition.	Des contrôles sont utilisés pour protéger les authentificateurs des attaques par répétition.
AC-10	Les attaques par voie latérale devraient être identifiées au moyen d'une évaluation des risques réalisée par le fournisseur CSP.	Les évaluations des risques pertinentes sont réalisées par le fournisseur CSP.

Tableau 8-3 – Contrôles empêchant la compromission de l'authentificateur

AC-11	La communication entre le déclarant et le contrôleur (via le canal principal dans le cas d'un authentificateur hors bande) devrait être assurée au moyen d'un canal protégé authentifié.	La communication entre le déclarant et le contrôleur est protégée.
AC-12	Les dispositifs cryptographiques à un seul facteur utilisés au niveau AAL le plus élevé devraient être validés dans la mesure requise par un programme de vérification de module cryptographique approuvé.	La cryptographie de l'authentificateur est validée dans la mesure nécessaire pour atteindre le niveau AAL souhaité.
AC-13	Lorsqu'un dispositif de type smartphone est utilisé pour l'authentification, le déverrouillage de l'appareil (généralement à l'aide d'un numéro d'identification personnel (PIN) ou d'un paramètre biométrique) ne devrait pas être considéré comme un facteur d'authentification.	Les authentificateurs appropriés sont utilisés pour atteindre le niveau AAL souhaité.
AC-14	Le système biométrique ne devrait pas autoriser plus de 10 tentatives d'authentification infructueuses consécutives. Une fois cette limite atteinte, l'authentificateur biométrique devrait soit: • imposer un délai d'au moins 30 s avant la prochaine tentative, augmentant de façon exponentielle à chaque tentative successive (par exemple, 1 min avant l'échec de la tentative suivante, 2 min avant le deuxième échec); ou • désactiver l'authentification biométrique de l'utilisateur et proposer un autre facteur (par exemple, un autre paramètre biométrique ou un code PIN/mot de passe si ce n'est pas déjà un facteur requis) si une telle méthode alternative est déjà disponible.	Le système biométrique met en place des contrôles pour protéger les authentificateurs contre les attaques par devinette.

8.3 Compromission de la transaction

8.3.1 Risques de compromission de la transaction

La compromission de la transaction est une attaque qui perturbe la confidentialité ou la disponibilité des données en transit qui sont échangées entre deux parties. Les attaques susceptibles de compromettre les transactions sont les attaques dites par "homme du milieu" (MITM), "homme dans le navigateur" (MITB), écoute illicite et détournement de session.

8.3.2 Contrôles empêchant la compromission de la transaction

Le Tableau 8-4 dresse la liste des contrôles visant à empêcher la compromission de la transaction.

Tableau 8-4 – Contrôles empêchant la compromission de la transaction

CTRL #	Description du contrôle	Résultat attendu
TC-1	Dans les cas où le contrôleur et le fournisseur CSP sont deux entités séparées, les communications entre les deux entités devraient être assurées au moyen d'un canal sécurisé mutuellement authentifié (par exemple, une connexion TLS authentifiée par le client) utilisant une cryptographie approuvée.	Les communications entre le contrôleur et le fournisseur CSP sont protégées.
TC-2	Un secret de session devrait être partagé entre le logiciel de l'abonné et le service faisant l'objet d'un accès.	Les secrets de session sont mis en œuvre et protégés.
TC-3	Les localisateurs uniformes de ressources (URL) ou contenus HTTP POST [b-IETF RFC 7231] devraient comporter un identificateur de session qui devrait être vérifié par la partie utilisatrice pour garantir que les actions menées à l'extérieur de la session n'affectent pas la session protégée.	Les identificateurs de session sont vérifiés par la partie utilisatrice.
TC-4	Le secret devrait être présenté directement par le logiciel de l'abonné ou la possession du secret devrait être démontrée au moyen d'un mécanisme de cryptographie.	Les secrets de session sont générés aléatoirement, mis en œuvre de manière appropriée et éliminés de manière adéquate après utilisation.
TC-5	Les secrets utilisés pour les liaisons de session ne devraient pas être disponibles pour les communications non sécurisées entre l'hôte et le point d'extrémité de l'abonné. Les sessions, une fois authentifiées, ne doivent pas retomber sur un transport non sécurisé, par exemple de HTTPS (protocole de transfert hypertexte sécurisé) à HTTP (protocole de transfert hypertexte).	La transmission des secrets de session est protégée.
TC-6	Les secrets utilisés pour les liaisons de session devraient être générés par l'hôte de la session pendant une interaction, généralement immédiatement après l'authentification de l'utilisateur.	Les secrets de session sont générés aléatoirement, mis en œuvre de manière appropriée et éliminés de manière adéquate après utilisation.
TC-7	Les secrets utilisés pour les liaisons de session devraient être générés par un générateur aléatoire de bits et contenir au moins 64 bits d'entropie.	Les secrets de session sont générés aléatoirement, mis en œuvre de manière appropriée et éliminés de manière adéquate après utilisation.
TC-8	Les secrets utilisés pour les liaisons de session devraient être effacés ou invalidés par le sujet de la session lorsque l'utilisateur se déconnecte.	Les secrets de session sont générés aléatoirement, mis en œuvre de manière appropriée et éliminés de manière adéquate après utilisation.
TC-9	Les secrets utilisés pour les liaisons de session devraient être envoyés au dispositif utilisant un canal protégé authentifié et reçus par celui-ci.	La transmission des secrets de session est protégée.
TC-10	Les secrets utilisés pour les liaisons de session devraient expirer et ne pas être acceptés après la période définie par le fournisseur CSP.	La transmission des secrets de session est protégée.

Tableau 8-4 – Contrôles empêchant la compromission de la transaction

CTRL #	Description du contrôle	Résultat attendu
TC-11	Les secrets utilisés pour les liaisons de session devraient être générés par l'hôte de la session en réponse directe à un événement d'authentification.	Les secrets de session sont générés aléatoirement, mis en œuvre de manière appropriée et éliminés de manière adéquate après utilisation.
TC-12	Les cookies du navigateur devraient être identifiés pour être accessibles uniquement lors de sessions HTTPS.	La transmission des secrets de session est protégée.
TC-13	Les cookies du navigateur devraient être accessibles à l'ensemble pratique standard de noms de serveur et de trajets.	La transmission des secrets de session est protégée.
TC-14	La continuité des sessions authentifiées devrait être basée sur la possession d'un secret de session émis par le contrôleur au moment de l'authentification et éventuellement actualisé pendant la session.	Les secrets de session sont générés aléatoirement, mis en œuvre de manière appropriée et éliminés de manière adéquate après utilisation.
TC-15	Si la comparaison est effectuée de manière centralisée, les données biométriques devraient être transmises sur le canal protégé authentifié.	La transmission des informations biométriques est protégée.
TC-16	Un canal protégé authentifié entre le capteur (ou un point d'extrémité contenant un capteur résistant au remplacement) et le contrôleur devrait être établi.	Les communications entre le contrôleur et les points d'extrémité sont protégées.

8.4 Usurpation de l'identité du contrôleur

8.4.1 Risques d'usurpation de l'identité du contrôleur

L'usurpation de l'identité du contrôleur est une attaque dans laquelle une entité est incitée à interagir avec un faux contrôleur et frauduleusement conduite à révéler des informations relatives aux justificatifs. Les informations ainsi obtenues par l'auteur d'une attaque peuvent représenter un risque important relevant des catégories de menaces liées à l'usurpation de l'identité de l'abonné ou à la compromission des justificatifs d'identité. L'une des attaques les plus courantes associées à l'usurpation d'identité du contrôleur est l'hameçonnage. L'auteur d'une attaque peut inciter l'entité à transmettre des informations relatives aux justificatifs de l'abonné à un client, un serveur ou un service non fiable et utiliser les informations ainsi obtenues pour accéder sans autorisation au système d'information.

8.4.2 Contrôles empêchant l'usurpation de l'identité du contrôleur

Le Tableau 8-5 dresse la liste des contrôles visant à empêcher l'usurpation de l'identité du contrôleur.

Tableau 8-5 – Contrôles empêchant l'usurpation de l'identité du contrôleur

CTRL #	Description du contrôle	Résultat attendu
VI-1	Les contrôleurs devraient être validés pour répondre aux exigences du programme de vérification de module cryptographique approuvé.	La cryptographie approuvée est utilisée.

Tableau 8-5 – Contrôles empêchant l'usurpation de l'identité du contrôleur

CTRL #	Description du contrôle	Résultat attendu
VI-2	Un protocole d'authentification résistant à l'usurpation de l'identité du contrôleur devrait établir un canal protégé authentifié avec le contrôleur.	Le résultat de l'authentificateur est protégé.
VI-3	Un canal protégé authentifié devrait relier, de manière forte et irréversible, un identificateur de canal négocié pour l'établissement de ce canal et le résultat de l'authentificateur.	Le résultat de l'authentificateur est protégé.
VI-4	Le contrôleur devrait valider la signature ou d'autres informations utilisées pour prouver la résistance à l'usurpation de l'identité du contrôleur.	Les contrôleurs procèdent à la validation avec efficacité.
VI-5	Des algorithmes cryptographiques approuvés devraient être utilisés pour établir la résistance à l'usurpation de l'identité du contrôleur lorsque cela est requis.	La cryptographie approuvée est utilisée.
VI-6	Les clés utilisées pour augmenter la résistance à l'usurpation de l'identité du contrôleur devraient fournir *a minima* le niveau de sécurité le plus bas spécifié dans une norme cryptographique en vigueur.	Il n'y a pas d'usurpation de l'identité des contrôleurs.
VI-7	Pour être considérées comme résistantes à l'usurpation de l'identité du contrôleur, les clés publiques stockées par le contrôleur devraient être associées à l'utilisation d'algorithmes cryptographiques approuvés et devraient fournir *a minima* le niveau de sécurité le plus bas spécifié dans une norme cryptographique en vigueur.	Il n'y a pas d'usurpation de l'identité des contrôleurs.
VI-8	Les secrets résistants à l'usurpation de l'identité du contrôleur devraient utiliser des algorithmes de hachage approuvés et les secrets sous-jacents devraient présenter *a minima* le niveau de sécurité le plus bas spécifié dans une norme cryptographique en vigueur.	Il n'y a pas d'usurpation de l'identité des contrôleurs.
VI-9	Les authentificateurs qui impliquent l'entrée manuelle du résultat, tels que les authentificateurs hors bande et OTP, ne doivent pas être considérés comme résistants à l'usurpation de l'identité du contrôleur, car l'entrée manuelle ne lie pas le résultat de l'authentificateur à la session spécifique en cours d'authentification.	Les authentificateurs requérant une entrée manuelle ne servent pas à protéger contre l'usurpation de l'identité du contrôleur.

8.5 Usurpation de l'identité de l'abonné

8.5.1 Risques d'usurpation de l'identité de l'abonné

L'usurpation de l'identité de l'abonné est une attaque impliquant la falsification d'une identité légitime pour compromettre la procédure d'authentification et accéder sans autorisation à un réseau ou système

d'information. Les attaques par usurpation d'identité de l'abonné les plus courantes sont le spoofing et le détournement de session. Dans le cadre d'une attaque par spoofing, l'auteur de l'attaque, qui souhaite usurper l'identité de la partie utilisatrice, peut simuler l'adresse MAC (commande d'accès au support) d'un dispositif authentifié pour accéder sans autorisation au réseau. L'auteur de l'attaque peut aussi usurper l'identité d'un utilisateur légitime en présentant des preuves falsifiées ou volées et utiliser un protocole de réinitialisation des justificatifs.

8.5.2 Contrôles empêchant l'usurpation de l'identité de l'abonné

Le Tableau 8-6 dresse la liste des contrôles visant à empêcher l'usurpation de l'identité de l'abonné.

Tableau 8-6 – Contrôles empêchant l'usurpation de l'identité de l'abonné

CTRL #	Description du contrôle	Résultat attendu
SI-1	La procédure d'authentification utilise un identificateur qui doit être utilisé à chaque fois qu'un abonné s'authentifie auprès de la partie utilisatrice.	Le ou les authentificateurs sont liés à l'abonné approprié.
SI-2	Pour satisfaire aux exigences d'un niveau AAL donné, le déclarant doit être authentifié avec au moins un niveau de protection donné pour être reconnu comme abonné.	L'abonné est authentifié au moyen du ou des authentificateurs appropriés avec le bon niveau de protection pour atteindre le niveau AAL souhaité.
SI-3	Toutes les procédures d'authentification et de réauthentification devraient démontrer l'intention d'authentification d'au moins un authentificateur.	L'intention de l'authentificateur est démontrée.
SI-4	Les fournisseurs CSP devraient fournir aux abonnés des instructions sur la manière de protéger efficacement l'authentificateur contre le vol ou la perte.	L'abonné est en mesure de récupérer un ou plusieurs authentificateurs sans contourner le niveau AAL souhaité.
SI-5	L'authentification au niveau AAL le plus bas devrait utiliser l'un des types d'authentificateur suivants: • secret mémorisé • secret de recherche • dispositif hors bande • dispositif OTP à un seul facteur • dispositif OTP à plusieurs facteurs • logiciel cryptographique à un seul facteur • dispositif cryptographique à un seul facteur • logiciel cryptographique à plusieurs facteurs • dispositif cryptographique à plusieurs facteurs	L'abonné est authentifié au moyen du ou des authentificateurs appropriés avec le bon niveau de protection pour atteindre le niveau AAL souhaité.

Tableau 8-6 – Contrôles empêchant l'usurpation de l'identité de l'abonné

CTRL #	Description du contrôle	Résultat attendu
SI-6	L'authentification au niveau AAL supérieur devrait utiliser soit un authentificateur à plusieurs facteurs soit une combinaison de deux authentificateurs à un seul facteur. Dans le cas d'un authentificateur à plusieurs facteurs, on pourra utiliser n'importe lesquels il peut s'agir de l'un des éléments suivants: • dispositif OTP à plusieurs facteurs • logiciel cryptographique à plusieurs facteurs • dispositif cryptographique à plusieurs facteurs	L'abonné est authentifié au moyen du ou des authentificateurs appropriés avec le bon niveau de protection pour atteindre le niveau AAL souhaité.
SI-7	Dans le cas d'une combinaison de deux authentificateurs à un seul facteur, il peut s'agir d'un authentificateur secret mémorisé et d'un authentificateur basé sur la possession ("une chose que possède l'entité") figurant dans la liste suivante: • secret de recherche • dispositif hors bande • dispositif OTP à un seul facteur • logiciel cryptographique à un seul facteur • dispositif cryptographique à un seul facteur	L'abonné est authentifié au moyen du ou des authentificateurs appropriés avec le bon niveau de protection pour atteindre le niveau AAL souhaité.
SI-8	L'authentification au niveau AAL le plus élevé devrait utiliser une combinaison d'authentificateurs. Les combinaisons possibles sont établies à partir des éléments suivants: • dispositif cryptographique à plusieurs facteurs • dispositif cryptographique à un seul facteur avec secret mémorisé • dispositif OTP à plusieurs facteurs – logiciel ou matériel – avec dispositif cryptographique à un seul facteur • dispositif OTP à plusieurs facteurs – matériel seulement – avec logiciel cryptographique à un seul facteur • dispositif OTP à un seul facteur – matériel seulement – avec authentificateur logiciel cryptographique à plusieurs facteurs • dispositif OTP à un seul facteur – matériel seulement – avec authentificateur logiciel cryptographique à un seul facteur et secret mémorisé	L'abonné est authentifié au moyen du ou des authentificateurs appropriés avec le bon niveau de protection pour atteindre le niveau AAL souhaité.
SI-9	Le fournisseur CSP devrait mettre à disposition un mécanisme pour révoquer ou suspendre l'authentificateur dès notification par l'abonné de la suspicion de perte ou de vol de l'authentificateur.	Des authentificateurs non valides ne peuvent pas être utilisés pour authentifier avec succès un individu.

Tableau 8-6 – Contrôles empêchant l'usurpation de l'identité de l'abonné

CTRL #	Description du contrôle	Résultat attendu
SI-10	Pour faciliter le signalement sécurisé de la perte, du vol ou des dommages à un authentificateur, le fournisseur CSP devrait fournir à l'abonné une méthode lui permettant de s'authentifier au moyen d'un authentificateur de sauvegarde ou de remplacement. Cet authentificateur de sauvegarde peut être soit un secret mémorisé soit un authentificateur physique.	L'abonné est en mesure de récupérer un ou plusieurs authentificateurs sans contourner le niveau AAL souhaité.
SI-11	La suspension peut être levée si l'abonné réussit à s'authentifier auprès du fournisseur CSP avec un authentificateur valide (non suspendu) et s'il demande la réactivation d'un authentificateur ainsi suspendu.	L'abonné est en mesure de récupérer un ou plusieurs authentificateurs sans contourner le niveau AAL souhaité.
SI-12	Un authentificateur qui arrive à expiration ne devrait pas être utilisable pour l'authentification.	Des authentificateurs non valides ne peuvent pas être utilisés pour authentifier avec succès un individu.
SI-13	Le fournisseur CSP devrait exiger des abonnés qu'ils restituent ou détruisent tout authentificateur physique contenant des certificats d'attribut qu'il aurait lui-même signés, dès que possible après invalidation de l'authentificateur par expiration, par révocation, par résiliation, par renouvellement ou par tout autre moyen défini par le fournisseur.	Des authentificateurs non valides ne peuvent pas être utilisés pour authentifier avec succès un individu.
SI-14	Les fournisseurs CSP devraient révoquer sans délai le lien entre les authentificateurs lorsqu'une identité en ligne cesse d'exister, lorsque l'abonné en fait la demande ou lorsque le fournisseur CSP estime que l'abonné ne remplit plus les conditions d'éligibilité.	Des authentificateurs non valides ne peuvent pas être utilisés pour authentifier avec succès un individu.
SI-15	La biométrie ne doit être utilisée que dans le cadre d'une authentification à plusieurs facteurs avec un authentificateur physique (une chose que possède l'entité).	La biométrie est utilisée de manière appropriée comme authentificateur.
SI-16	Au niveau AAL supérieur, le fournisseur CSP devrait relier au moins un, et devrait relier au moins deux, authentificateurs physiques (une chose que possède l'entité) avec l'identité en ligne d'un abonné, en plus d'un secret mémorisé ou d'une ou plusieurs données biométriques.	Le ou les authentificateurs sont liés à l'abonné approprié.

Tableau 8-6 – Contrôles empêchant l'usurpation de l'identité de l'abonné

CTRL #	Description du contrôle	Résultat attendu
SI-17	Au niveau AAL supérieur, si l'inscription et la liaison ne peuvent pas être effectuées au cours d'une seule rencontre physique ou transaction électronique, il conviendrait d'utiliser les méthodes suivantes pour garantir que c'est bien la même partie qui agit en tant que déclarant tout au long du processus: Pour les transactions à distance: 1) Le déclarant devrait s'identifier lors de chaque nouvelle transaction en présentant un secret temporaire qui a été établi lors d'une précédente transaction ou envoyé sur le numéro de téléphone, l'adresse e-mail ou l'adresse postale d'enregistrement du déclarant. 2) Les secrets d'authentificateur à long terme ne devraient être délivrés au déclarant que dans le cadre d'une session protégée. Pour les transactions en présence: 1) Le déclarant devrait s'identifier en personne, soit en utilisant un secret tel que décrit au point 1 de l'alinéa précédent relatif aux transactions à distance, soit en utilisant un paramètre biométrique enregistré lors d'une rencontre antérieure. 2) Les secrets temporaires ne devraient pas être réutilisés. 3) Si le fournisseur CSP délivre des secrets d'authentification à long terme lors d'une transaction physique, ceux-ci devraient être chargés localement sur un appareil physique qui est délivré en personne au déclarant ou remis d'une manière qui confirme l'adresse d'enregistrement.	Le ou les authentificateurs sont liés à l'abonné approprié.
SI-18	Lors de la liaison d'un authentificateur supplémentaire au compte d'un abonné, le fournisseur CSP devrait d'abord demander à l'abonné de s'authentifier au moins au niveau AAL sur lequel le nouvel authentificateur sera utilisé.	Le ou les authentificateurs sont liés à l'abonné approprié.
SI-19	Au niveau AAL supérieur, si un abonné perd tous les authentificateurs d'un facteur nécessaire pour terminer l'authentification à plusieurs facteurs, cet abonné doit répéter le processus de vérification d'identité.	L'abonné est en mesure de récupérer un ou plusieurs authentificateurs sans contourner le niveau AAL souhaité.

Tableau 8-6 – Contrôles empêchant l'usurpation de l'identité de l'abonné

CTRL #	Description du contrôle	Résultat attendu
SI-20	Lors du remplacement d'un facteur d'authentification perdu pour un niveau AAL supérieur, le fournisseur CSP devrait demander au déclarant de s'authentifier au moyen d'un authentificateur de n'importe quel facteur restant, pour confirmer le lien avec l'identité existante.	L'abonné est en mesure de récupérer un ou plusieurs authentificateurs sans contourner le niveau AAL souhaité.
SI-21	Les sessions devraient être réauthentifiées de manière périodique pour confirmer la présence continue de l'abonné à une session authentifiée.	Il est demandé à l'abonné de se réauthentifier périodiquement avec le ou les authentificateurs appropriés et avec le bon niveau de protection pour atteindre le niveau AAL souhaité.
SI-22	Les sessions d'abonné devraient être réauthentifiées de manière périodique. a) Au niveau AAL le plus bas, la réauthentification de l'abonné devrait être répétée au moins une fois tous les 30 jours pendant une session d'utilisation prolongée, quelle que soit l'activité de l'utilisateur. b) Au niveau AAL le plus bas, la session devrait être terminée (c'est-à-dire déconnectée) lorsque cette limite de temps est atteinte. c) Au niveau AAL supérieur, la réauthentification de l'abonné devrait être répétée au moins une fois toutes les 12 h pendant une session d'utilisation prolongée, quelle que soit l'activité de l'utilisateur. d) Au niveau AAL supérieur, la réauthentification de l'abonné devrait être répétée après toute période d'inactivité de 30 min ou plus. e) Au niveau AAL supérieur, la session devrait être terminée (c'est-à-dire déconnectée) lorsque l'une de ces deux limites de temps est atteinte. f) Au niveau AAL le plus élevé, la réauthentification de l'abonné devrait être répétée au moins une fois toutes les 12 h pendant une session d'utilisation prolongée, quelle que soit l'activité de l'utilisateur. g) Au niveau AAL le plus élevé, la réauthentification de l'abonné devrait être répétée après toute période d'inactivité de 15 min ou plus. h) Au niveau AAL le plus élevé, la session devrait être terminée (c'est-à-dire déconnectée) lorsque l'une des limites de temps (f) ou (g) est atteinte.	Il est demandé à l'abonné de se réauthentifier périodiquement avec le ou les authentificateurs appropriés et avec le bon niveau de protection pour atteindre le niveau AAL souhaité.

Tableau 8-6 – Contrôles empêchant l'usurpation de l'identité de l'abonné

CTRL #	Description du contrôle	Résultat attendu
	i) Au niveau AAL le plus élevé, les sessions d'abonné devraient être réauthentifiées de manière périodique en utilisant les facteurs d'authentification d'origine.	
SI-23	Une session ne devrait pas être prolongée uniquement sur la base de la présentation du secret de la session.	Il est demandé à l'abonné de se réauthentifier périodiquement avec le ou les authentificateurs appropriés et avec le bon niveau de protection pour atteindre le niveau AAL souhaité.
SI-24	Lorsqu'une session est terminée, en raison d'un délai d'expiration ou d'une autre action, il devrait être demandé à l'utilisateur d'établir une nouvelle session en s'authentifiant à nouveau.	Il est demandé à l'abonné de se réauthentifier périodiquement avec le ou les authentificateurs appropriés et avec le bon niveau de protection pour atteindre le niveau AAL souhaité.
SI-25	Les secrets de session devraient être non persistants. Autrement dit, ils ne devraient pas être conservés lors d'un redémarrage de l'application associée ou d'un reboot du dispositif hôte.	Il est demandé à l'abonné de se réauthentifier périodiquement avec le ou les authentificateurs appropriés et avec le bon niveau de protection pour atteindre le niveau AAL souhaité.

8.6 Risques et contrôles empêchant la compromission du service d'authentification

8.6.1 Risques empêchant la compromission du service d'authentification

La compromission du service d'authentification est une attaque contre l'entité fournissant le service d'identité, qui la rend invalide, inexacte, indisponible ou incapable de fonctionner comme prévu. Chaque point de faiblesse dans l'environnement de contrôle du système d'information d'une entité peut être exploité pour compromettre le service d'authentification. L'auteur d'une attaque peut ainsi exploiter une vulnérabilité logicielle non corrigée et obtenir par ce biais un accès privilégié non autorisé au système d'information du service d'authentification.

8.6.2 Contrôles empêchant la compromission du service d'authentification

Le Tableau 8-7 dresse la liste des contrôles visant à empêcher la compromission du service d'authentification.

Tableau 8-7 – Contrôles empêchant la compromission du service d'authentification

CTRL #	Description du contrôle	Résultat attendu
ASC-1	Les fournisseurs CSP devraient utiliser des contrôles de sécurité adaptés pour un niveau de sécurité donné tel que précisé dans [b-ISO/CEI 27002] ou une norme équivalente.	L'intégrité du service d'authentification est protégée contre la compromission.
ASC-2	Les fournisseurs CSP devraient veiller à ce que les contrôles minimaux de garantie soient respectés dans le contexte du risque global pesant sur le système.	L'intégrité du service d'authentification est protégée contre la compromission.

Tableau 8-7 – Contrôles empêchant la compromission du service d'authentification

CTRL #	Description du contrôle	Résultat attendu
ASC-3	Si la comparaison est effectuée de manière centralisée, la révocation biométrique – appelée protection de gabarit biométrique dans [b-ISO/CEI 24745] – devrait être mise en œuvre.	Le service d'authentification protège les informations biométriques.
ASC-4	L'intention d'authentification devrait être établie par l'authentificateur lui-même, même si les dispositifs cryptographiques à plusieurs facteurs peuvent établir l'intention en rentrant l'autre facteur d'authentification sur le point d'extrémité où l'authentificateur est utilisé.	L'intention d'authentification n'est établie que par l'authentificateur.
ASC-5	Pendant toute la durée du cycle de vie de l'identité numérique, les fournisseurs CSP devraient tenir à jour un registre de tous les authentificateurs qui sont ou ont été associés à chaque identité.	Les informations d'authentification sont enregistrées et conservées.
ASC-6	Les fournisseurs CSP ou contrôleurs devraient également conserver les informations requises pour limiter les tentatives d'authentification si nécessaire.	Les informations d'authentification sont enregistrées et conservées.
ASC-7	Le registre établi par les fournisseurs CSP devrait contenir la date et l'heure à laquelle l'authentificateur a été associé au compte.	Les informations d'authentification sont enregistrées et conservées.
ASC-8	Les authentificateurs devraient être liés aux comptes d'abonné: • via la publication par le fournisseur CSP dans le cadre de l'inscription; ou • via l'association d'un authentificateur fourni par l'abonné considéré comme acceptable par le fournisseur CSP.	Les authentificateurs sont liés de manière appropriée aux comptes d'abonné.
ASC-9	Lorsqu'un nouvel authentificateur est lié à un compte d'abonné, le fournisseur CSP doit s'assurer que les protocoles de liaison et de mise à disposition de la ou des clés associées correspondent à un niveau de sécurité proportionné au niveau AAL sur lequel l'authentificateur sera utilisé.	Les authentificateurs sont liés de manière appropriée aux comptes d'abonné.
ASC-10	La liaison d'authentificateurs à plusieurs facteurs devrait nécessiter une authentification multifactorielle ou une association avec la session dans laquelle la vérification d'identité vient d'être réalisée afin de lier l'authentificateur.	Les authentificateurs sont liés de manière appropriée aux comptes d'abonné.

8.7 Risques et contrôles liés à la protection de la vie privée

8.7.1 Risques liés à la protection de la vie privée

L'authentification numérique renforce la protection de la vie privée en atténuant les risques d'accès non autorisé aux informations des individus. Sachant que les procédures de vérification d'identité,

d'authentification, d'autorisation et de fédération impliquent le traitement d'informations de nature privée, il peut aussi en résulter des risques pour la vie privée. Les présentes lignes directrices incluent par conséquent des exigences et des considérations en matière de vie privée pour aider à atténuer les risques potentiels de confidentialité associés.

Le fournisseur CSP doit procéder à une évaluation des risques concernant les données personnelles à des fins de conservation des enregistrements. Cette évaluation peut inclure les éléments suivants:

1) La probabilité que la conservation des enregistrements puisse créer un problème pour l'abonné, tel qu'un caractère invasif ou un accès non autorisé aux informations.

2) L'impact qui pourrait en découler si ce problème s'avère réel.

Les fournisseurs CSP devraient être en mesure de justifier raisonnablement toute réponse adoptée face aux risques identifiés pour la vie privée, y compris l'acceptation du risque, l'atténuation du risque et le partage du risque. L'utilisation du consentement de l'abonné est une forme de partage du risque et ne peut, à ce titre, être utilisée que si l'on peut raisonnablement s'attendre à ce que l'abonné ait la capacité d'évaluer et d'accepter le risque partagé.

8.7.2 Contrôles liés à la protection de la vie privée

Le Tableau 8-8 dresse la liste des contrôles liés à la protection de la vie privée.

Tableau 8-8 – Contrôles liés à la protection de la vie privée

CTRL #	Description du contrôle	Résultat attendu
P-1	Un fournisseur IDP devrait sélectionner au moins un niveau AAL approprié lorsque des informations PII auto-affirmées ou autres informations personnelles sont rendues accessibles en ligne.	Le fournisseur CSP applique les politiques et contrôles de confidentialité en ce qui concerne l'authentification.
P-2	Le fournisseur CSP devrait se conformer à ses politiques respectives de conservation des enregistrements conformément aux lois, réglementations et politiques applicables le cas échéant. S'il choisit de conserver les enregistrements en l'absence d'exigences réglementaires, le fournisseur CSP devrait appliquer une procédure de gestion des risques, incluant une évaluation des risques en termes de vie privée et de sécurité, pour déterminer la durée de conservation des enregistrements et devrait informer l'abonné de cette politique de conservation.	Le fournisseur CSP authentifie les abonnés conformément aux lois, réglementations et politiques.
P-3	Des précautions devraient être prises pour s'assurer que l'utilisation des informations PII est limitée à son objectif initial de collecte.	Le fournisseur CSP collecte le minimum d'informations PII pour atteindre le niveau AAL souhaité.
P-4	Si l'utilisation des informations PII dépasse le cadre des prescriptions requises pour l'authentification ou la conformité aux lois et procédures légales, le fournisseur CSP devrait adresser une note d'information et obtenir le consentement de l'abonné.	Le fournisseur CSP authentifie les abonnés conformément aux lois, réglementations et politiques.

Tableau 8-8 – Contrôles liés à la protection de la vie privée

CTRL #	Description du contrôle	Résultat attendu
P-5	Le fournisseur IDP devrait réaliser ou publier une évaluation des incidences sur la vie privée (PIA) concernant la collecte des informations PII et autres informations personnelles, conformément aux lois et procédures légales.	Le fournisseur CSP réalise une évaluation PIA.
P-6	Le fournisseur CSP ne devrait pas utiliser ou divulguer des informations sur les abonnés à des fins autres que l'authentification, l'atténuation de la fraude qui en découle ou pour se conformer à la loi ou à une procédure juridique, à moins qu'il ne fournisse une information claire et n'obtienne le consentement de l'abonné pour des utilisations supplémentaires.	Le fournisseur CSP authentifie les abonnés conformément aux lois, réglementations et politiques.
P-7	Le fournisseur CSP devrait utiliser des contrôles de confidentialité adaptés, précisés dans [ISO/CEI 27002] ou une norme équivalente.	Le fournisseur CSP applique les politiques et contrôles de confidentialité en ce qui concerne l'authentification.
P-8	Le fournisseur CSP ne devrait pas faire du consentement une condition du service.	Le fournisseur CSP authentifie les abonnés conformément aux lois, réglementations et politiques.
P-9	Bien qu'un fournisseur CSP puisse lier un authentificateur AAL de niveau inférieur à une identité AAL de niveau supérieur, si l'abonné est authentifié au niveau AAL inférieur, le fournisseur CSP ne devrait pas exposer des informations personnelles, même auto-affirmées, à l'abonné.	Le fournisseur CSP collecte le minimum d'informations PII ou autres informations personnelles pour atteindre le niveau AAL souhaité.
P-10	L'acceptation par l'abonné d'utilisations supplémentaires ne devrait pas être une condition pour fournir des services d'authentification.	Le fournisseur CSP authentifie les abonnés conformément aux lois, réglementations et politiques.

Appendice I

Exemple d'authentification forte utilisant [b-UIT-T X.1278]

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

I.1 Introduction

Les documents *Cadre d'authentification universelle [b-UIT-T X.1277]* et *Protocole client-authentificateur/Cadre applicable au double facteur universel [b-UIT-T X.1278]* présentent des approches d'authentification et de garantie d'authentification qui fournissent une authentification forte basée sur des Recommandations ouvertes et interopérables. Le présent appendice donne un exemple d'authentification forte utilisant [b-UIT-T X.1278].

I.2 Catégories de menaces

La Figure I.1 classe les menaces en deux catégories:

1) Attaques graduelles – Quel que soit le nombre de cibles (1 000 ou 1 000 000), les coûts de l'attaque ne seront pas impactés.
    a) Attaques à distance de serveurs et vol de mots de passe. Ce type d'attaque est très sérieux dans la mesure où les utilisateurs ne peuvent pas se protéger – c'est aux parties utilisatrices de le faire. Les utilisateurs peuvent en revanche aggraver la situation: s'ils partagent les mots de passe entre plusieurs parties utilisatrices, la partie utilisatrice la moins sécurisée pourrait être piratée et affecter ainsi les autres parties.
    b) Attaques à distance de nombreux dispositifs d'utilisateur. Par exemple, tentative de vol de données depuis un dispositif dans le but d'usurper l'identité de l'utilisateur.
    c) Les attaques à distance peuvent également conduire à une utilisation abusive des données de dispositifs d'utilisateur à des fins d'usurpation d'identité des utilisateurs.
    d) Attaques à distance de nombreux dispositifs d'utilisateur en vue de l'utilisation abusive d'une session fortement authentifiée. Il s'agit d'une attaque MITB.

Il est intéressant de noter que les cartes à puce ne suffisent pas à protéger contre l'utilisation abusive des justificatifs, dans la mesure où elles ne peuvent pas savoir si le code PIN a été saisi par l'utilisateur ou injecté par un logiciel malveillant qui aurait précédemment hameçonné le code PIN de l'utilisateur.

2) Attaques physiques – lorsqu'un accès physique au dispositif est requis. Les attaques physiques ne sont pas des attaques graduelles, car le vol de smartphones (actifs) occasionne des coûts importants par cible.
    a) Attaques physiques de dispositifs d'utilisateur pour voler des données à des fins d'usurpation d'identité.
    b) Attaques physiques de dispositifs d'utilisateur pour les utiliser abusivement à des fins d'usurpation d'identité.

I.3 [b-UIT-T X.1278] offre une "authentification forte avec un niveau de garantie élevé"

Une authentification forte avec un niveau de garantie élevé implique:

1) d'utiliser deux facteurs ou plus;
2) qu'au moins un facteur s'appuie sur une cryptographie à clé publique
3) de résister à l'hameçonnage, aux attaques MITM ou autres attaques ciblant les justificatifs.

L'approche FIDO (authentification rapide en ligne) présente les caractéristiques clés suivantes:

- pas de secrets partagés – l'entité utilise ce qu'elle possède (par exemple, dispositifs matériels) et ce qu'elle est (par exemple, empreintes);

- utilisation d'une cryptographie à clé publique à la place de secrets partagés symétriques;
- l'utilisateur est vérifié par un authentificateur, et l'authentificateur s'authentifie auprès de la partie utilisatrice; et
- authentification à plusieurs facteurs résistante au hameçonnage.

Ces approches respectent les principes de sécurité et de confidentialité suivants:

- pas de possibilité de relier les services ou les comptes;
- pas de tierce partie dans le protocole;
- les données biométriques, si elles sont utilisées, ne quittent jamais le dispositif;
- les clés cryptographiques restent sur le dispositif;
- pas de secrets partagés du côté du serveur; et
- utilisation d'une cryptographie à clé publique.

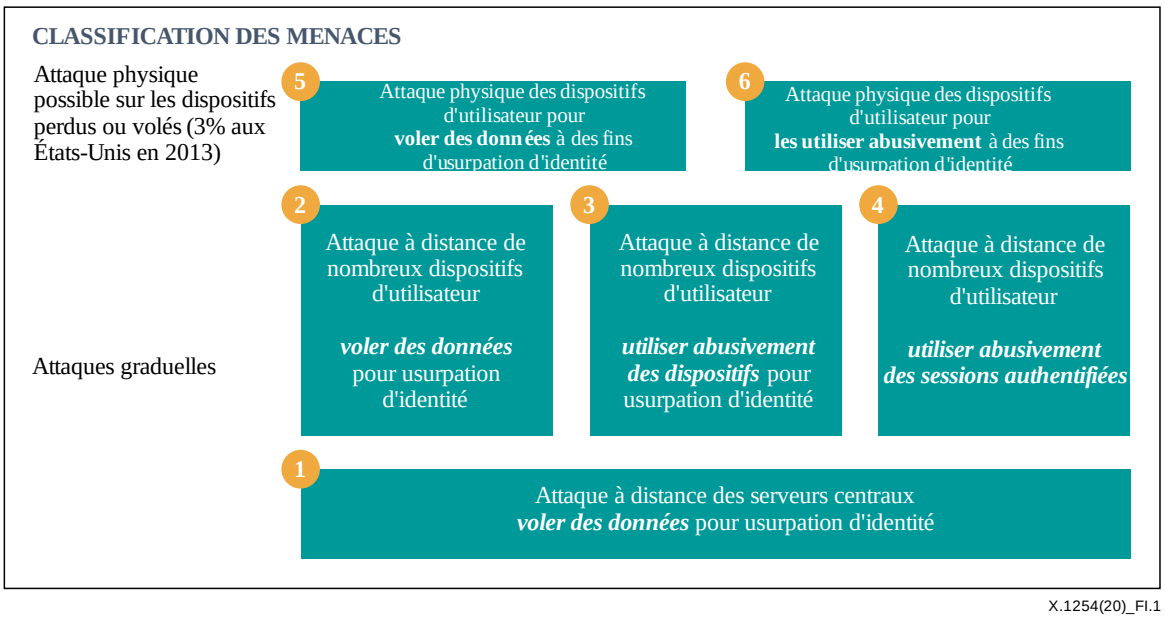

Figure I.1 – Classification des menaces

I.4 Ancienne authentification avec mots de passe

La procédure traditionnelle d'authentification par mot de passe présente plusieurs risques inhérents, comme le montre la Figure I.2.

1) Les mots de passe peuvent être volés depuis le serveur (violation de données).
2) Les mots de passe peuvent être saisis dans des applications ou sites web non sécurisés (hameçonnage).
3) Les mots de passe sont trop nombreux à mémoriser et sont donc réutilisés de plus en plus souvent (il devient plus facile de deviner les mots de passe d'un site à l'autre).
4) Les mots de passe sont difficiles à saisir sur les téléphones (les utilisateurs sélectionnent des mots de passe faciles à deviner).

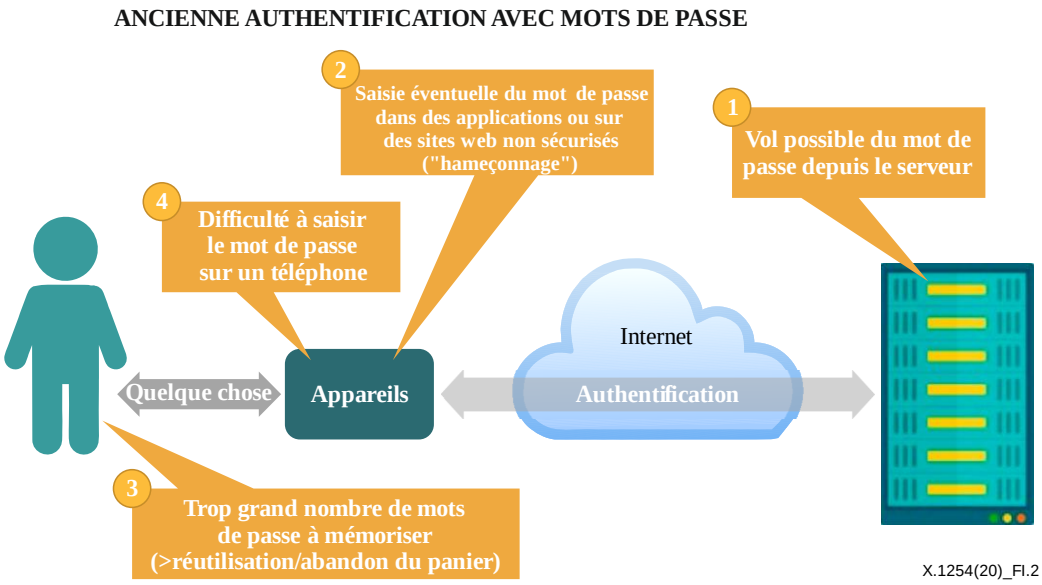

Figure I.2 – Ancienne authentification avec mots de passe

I.5 Nouvelle authentification avec [b-UIT-T X.1278]

FIDO sépare les aspects d'authentification et d'identité. La Figure I.3 montre les avantages de cette approche.

1) Les secrets ne sont pas sauvegardés sur le serveur (protection contre les violations de données).

2) Les authentificateurs ne peuvent pas être trompés par l'hameçonnage.

3) Pas de mot de passe à mémoriser et pas de frottement supplémentaire au niveau de la procédure d'authentification.

4) Commodité d'un seul geste à réaliser pour l'utilisateur.

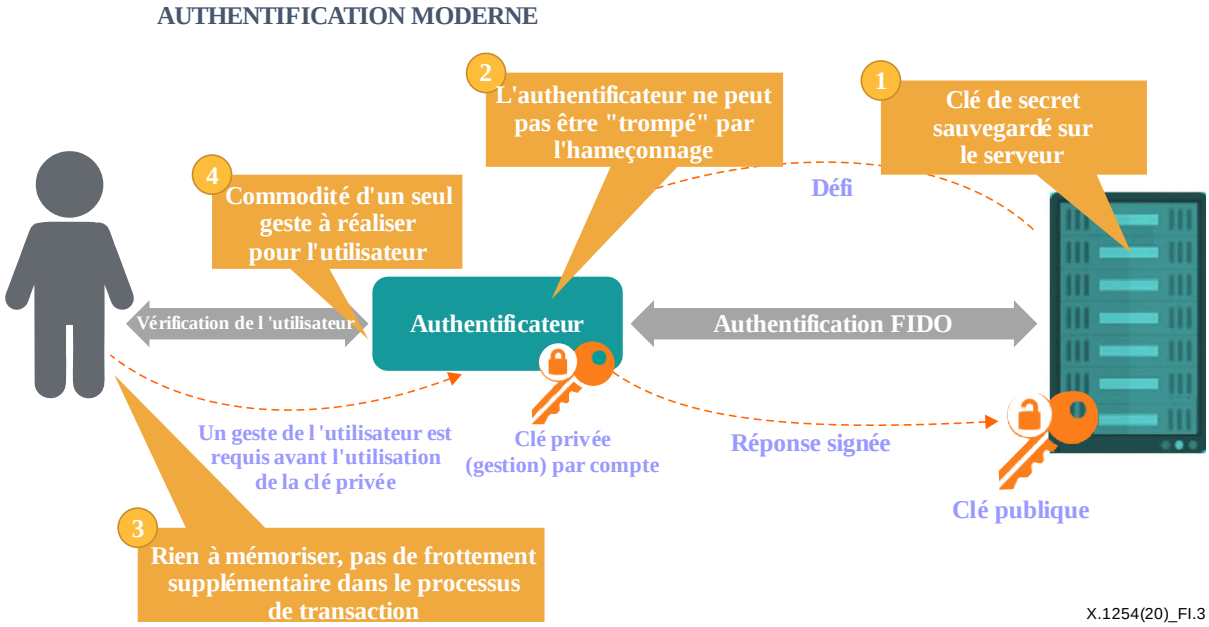

Figure I.3 – Nouvelle authentification avec [b-UIT-T X.1278]

I.6 Interopérabilité et certification

En plus de créer de nouvelles méthodes d'authentification, la force des solutions d'authentification est augmentée via l'interopérabilité et les tests de certification.

- Renforcement de l'acceptation de l'utilisateur ou du consommateur pour une authentification forte.
- Diminution du risque et de l'impact du vol d'identité grâce au déploiement généralisé d'une authentification forte.
- Commodité et amélioration de l'expérience utilisateur grâce à une large gamme de dispositifs et de services d'authentification.
- La réduction des coûts encourage l'adoption d'une authentification forte.

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

[b-UIT-T X.1277] Recommandation UIT-T X.1277 (2018), *Cadre d'authentification universelle.*

[b-UIT-T X.1278] Recommandation UIT-T X.1278 (2018), *Protocole client-authentificateur/Cadre applicable au double facteur universel*.

[b-ISO/CEI 18014-2] ISO/CEI 18014-2:2009, *Technologies de l'information – Techniques de sécurité – Services d'horodatage – Partie 2: mécanismes produisant des jetons indépendants.*

[b-ISO/CEI 19790] ISO/CEI 19790:2012, *Technologies de l'information – Techniques de sécurité – Exigences de sécurité pour les modules cryptographiques.*

[b-ISO/CEI 24745] ISO/CEI 24745:2011, *Technologies de l'information – Techniques de sécurité – Protection des informations biométriques.*

[b-ISO/CEI 24760-1] ISO/CEI 24760-1:2019, *Sécurité IT et confidentialité – Cadre pour la gestion de l'identité – Partie 1: Terminologie et concepts*

[b-ISO/CEI 27000] ISO/CEI 27000 (2018), *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*.

[b-ISO/CEI 27002] ISO/CEI 27002:2013, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information.*

[b-ISO/CEI TS 29003] Spécification technique ISO/CEI TS 29003:2018, *Technologies de l'information – Techniques de sécurité – Vérification de l'identité.*

[b-ISO/CEI 29115] ISO/CEI 29115:2013, *Technologies de l'information – Techniques de sécurité – Cadre d'assurance de l'authentification d'entité.*

[b-IETF RFC 7231] IETF RFC 7231 (2014), *Hypertext transfer protocol (HTTP/1.1): Semantics and content.*

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2021