

Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1254

(09/2012)

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

Sécurité du cyberspace – 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	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589

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

Recommandation UIT-T X.1254

Cadre de garantie d'authentification des entités

Résumé

La Recommandation UIT-T X.1254 définit quatre niveaux de garantie d'authentification des entités (LoA1-LoA4) ainsi que les critères et menaces correspondant à chacun de ces quatre niveaux. En outre:

- elle spécifie un cadre de gestion des niveaux de garantie;
- 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 quatre niveaux de garantie à d'autres systèmes de garantie d'authentification; et
- elle donne des orientations quant à l'échange des résultats d'authentification reposant sur les quatre niveaux de garantie.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1254	2012-09-07	17

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.

Un texte similaire est publié en tant qu'ISO/CEI 29115. Il diffère de la présente Recommandation selon quatre points: 1) paragraphe 3.1.6: la définition de justificatif d'identité est différente et, dans la présente Recommandation, elle fait référence à la définition de la Recommandation UIT-T X.1252; 2) Tableau 10-1: l'ISO/CEI 29115 inclut un exemple d'usurpation qui consiste en l'utilisation illégale d'informations relatives à l'identité d'une autre entité; 3) paragraphe 10.2.2.1: l'ISO/CEI 29115 décrit le SSL comme exemple de canal sécurisé; 4) Dans la présente Recommandation, l'Annexe A, *Caractéristiques d'un justificatif d'identité*, est normative.

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

© UIT 2013

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

	Page
1	Domaine d'application 1
2	Références..... 1
3	Définitions 1
3.1	Termes définis ailleurs 1
3.2	Termes définis dans la présente Recommandation 2
4	Abréviations et acronymes 3
5	Conventions 4
6	Niveaux de garantie 4
6.1	Niveau de garantie 1 (LoA1) 5
6.2	Niveau de garantie 2 (LoA2) 6
6.3	Niveau de garantie 3 (LoA3) 6
6.4	Niveau de garantie 4 (LoA4) 7
6.5	Choix du niveau de garantie approprié..... 7
6.6	Mise en correspondance avec les niveaux LoA et interopérabilité 8
6.7	Echange des résultats d'authentification fondés sur les quatre niveaux LoA..... 9
7	Acteurs..... 10
7.1	Entité..... 10
7.2	Fournisseur de services de justificatifs d'identité 10
7.3	Autorité d'enregistrement 10
7.4	Partie utilisatrice 11
7.5	Contrôleur..... 11
7.6	Tierce partie de confiance 11
8	Phases du cadre de garantie d'authentification des entités 11
8.1	Phase d'inscription 11
8.2	Phase de gestion des justificatifs d'identité 15
8.3	Phase d'authentification des entités 17
9	Considérations de gestion et d'organisation..... 18
9.1	Etablissement du service 18
9.2	Conformité juridique et contractuelle..... 18
9.3	Dispositions financières..... 18
9.4	Gestion de la sécurité des informations et audit 18
9.5	Composantes extérieures de service 19
9.6	Infrastructure opérationnelle 19
9.7	Capacités opérationnelles d'évaluation..... 19
10	Menaces et contrôles..... 19
10.1	Menaces pour la phase d'inscription et contrôles applicables 19

	Page
10.2 Menaces pour la phase de gestion des justificatifs d'identité et contrôles applicables	22
10.3 Menaces pour la phase d'authentification et contrôles applicables	28
11 Critères de garantie de service	33
Annexe A – Caractéristiques d'un justificatif d'identité.....	34
Appendice I – Confidentialité et protection des informations d'identification personnelle.....	36

Introduction

De nombreuses transactions électroniques, au sein des systèmes employant les technologies de l'information et de la communication (TIC) ou entre ces systèmes, ont des besoins en matière de sécurité qui dépendent du niveau convenu ou spécifié de confiance dans les identités des entités concernées. Ces besoins peuvent inclure la protection des biens et des ressources contre un accès non autorisé, pouvant se faire au moyen d'un mécanisme de contrôle d'accès, et/ou le respect des obligations, pouvant être assuré par la tenue de journaux d'audit où sont inscrits les événements pertinents, journaux qui peuvent également servir à des fins de comptabilité et de taxation.

La Recommandation UIT-T X.1254 fournit un cadre de garantie d'authentification des entités. Par garantie, on entend dans la présente Recommandation la confiance placée dans l'ensemble des processus, des activités de gestion et des technologies permettant d'établir et de gérer l'identité d'une entité, qui sont employés dans les transactions d'authentification.

Aspects techniques		Aspects de gestion et d'organisation
Phase d'inscription	<ul style="list-style-type: none"> • Demande et lancement • Vérification d'identité et contrôle des informations d'identité 	<ul style="list-style-type: none"> • Tenue des registres/consignation • Enregistrement
Phase de gestion des justificatifs d'identité	<ul style="list-style-type: none"> • Etablissement des justificatifs d'identité • Prétraitement des justificatifs d'identité • Délivrance des justificatifs d'identité • Activation des justificatifs d'identité • Archivage des justificatifs d'identité 	<ul style="list-style-type: none"> • Suspension, révocation et/ou destruction des justificatifs d'identité • Renouvellement ou remplacement des justificatifs d'identité • Tenue des registres
Phase d'authentification des entités	<ul style="list-style-type: none"> • Authentification • Tenue des registres 	<ul style="list-style-type: none"> • Etablissement du service • Conformités juridique et contractuelle • Dispositions financières • Gestion de la sécurité des informations et audit • Composantes extérieures de service • Infrastructure opérationnelle • Capacités opérationnelles d'évaluation

X.1254(12)_F01

Figure 1 – Aperçu du cadre de garantie d'authentification des entités

Sur la base de la spécification de quatre niveaux de garantie (LoA, *level of assurance*), la présente Recommandation donne des orientations en matière de techniques de contrôle, de processus et d'activités de gestion, ainsi que de critères de garantie, qui devraient être utilisées afin d'atténuer les menaces pour l'authentification et d'appliquer les quatre niveaux LoA. Elle donne aussi des orientations relatives à l'application des quatre niveaux spécifiés à d'autres systèmes de garantie d'authentification, ainsi que des orientations quant à l'échange des résultats d'une transaction d'authentification. Finalement, la présente Recommandation donne des orientations concernant la protection des informations d'identification personnelle (PII, *personally identifiable information*) associées à la procédure d'authentification.

La présente Recommandation est destinée à être utilisée principalement par les fournisseurs de services de justificatifs d'identité (CSP, *credential service provider*) et par ceux qui sont intéressés par leurs services (par exemple, les parties utilisatrices, les estimateurs et les vérificateurs de ces services). Ce cadre de garantie d'authentification des entités (EAAF, *entity authentication assurance framework*) spécifie les conditions minimales à remplir, sur le plan technique, sur le plan de la gestion et sur le plan du traitement pour les quatre niveaux LoA, afin de garantir l'équivalence des justificatifs d'identité délivrés par les différents fournisseurs CSP. Il contient aussi des

considérations supplémentaires de gestion et d'organisation, qui influent sur la garantie d'authentification des entités, mais il ne donne aucun critère spécifique les concernant. Les parties utilisatrices et d'autres trouveront peut-être la présente Recommandation utile en vue de mieux comprendre les garanties offertes par chacun des niveaux LoA. En outre, ce cadre de garantie peut servir à établir un climat de confiance pour définir les spécifications techniques relatives aux niveaux LoA. Le cadre EAAF est destiné, mais pas uniquement, à être utilisé dans des cas où importent la session ou le document et où interviennent diverses technologies d'authentification. S'agissant de la confiance, tant les scénarios directs que négociés sont possibles, dans le cadre d'arrangements juridiques/bilatéraux ou de fédérations.

Recommandation UIT-T X.1254

Cadre de garantie d'authentification des entités¹

1 Domaine d'application

La présente Recommandation fournit un cadre de gestion des garanties d'authentification des entités dans un contexte donné. En particulier:

- elle spécifie quatre niveaux de garantie d'authentification des entités;
- elle définit des critères et des lignes directrices permettant d'atteindre chacun des quatre niveaux de garantie d'authentification des entités (LoA, *level of assurance*);
- elle donne des orientations relatives à l'application des quatre niveaux LoA à d'autres systèmes de garantie d'authentification;
- elle donne des orientations quant à l'échange des résultats d'authentification, fondés sur les quatre niveaux LoA;
- elle donne des orientations concernant les contrôles qui devraient être exécutés pour atténuer les menaces pour l'authentification.

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]: garantie donnée concernant l'identité d'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, la signature d'un dispositif, un passeport, un dispositif matériel contenant un justificatif d'identité, une clé privée);
- une chose que connaît l'entité (par exemple, un mot de passe, le numéro d'identification personnel (PIN, *personal identification number*);
- une chose qu'est l'entité (par exemple, ses caractéristiques biométriques);
- une chose que fait généralement l'entité (par exemple, son attitude comportementale).

¹ La Corée (République de) a exprimé une réserve et n'appliquera pas la présente Recommandation car celle-ci n'est pas compatible avec la réglementation en vigueur dans ce pays en ce qui concerne les quatre niveaux requis de garantie d'authentification des entités et les critères permettant d'atteindre chacun de ces niveaux.

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

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

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

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

3.1.7 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.

3.1.8 identité [b-ISO/CEI 24760]: ensemble d'attributs se rapportant à une entité.

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.

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

3.1.10 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.

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

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 protocole d'authentification: séquence définie de messages entre une entité et un contrôleur, qui permet à celui-ci d'authentifier l'entité.

3.2.2 source faisant autorité: répertoire reconnu comme étant une source d'informations précises et mises à jour.

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

3.2.4 garantie d'authentification d'entité (EAA, *entity authentication 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 (définition établie à partir de la définition de la "garantie d'authentification" figurant dans [b-UIT-T X.1252]).

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

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

3.2.6 contrôle des informations d'identité: 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.

3.2.7 vérification d'identité: procédure au moyen de laquelle l'autorité d'enregistrement (RA, *registration authority*) recueille et contrôle un nombre suffisant d'informations pour identifier une entité à un niveau de garantie spécifié ou convenu.

3.2.8 attaque par hôte interposé: attaque au cours de laquelle un attaquant est capable de lire, d'insérer ou de modifier des messages entre deux parties, à leur insu.

3.2.9 authentification mutuelle: authentification des identités d'entités, qui donne à chacune des deux entités une garantie quant à l'identité de l'autre.

3.2.10 hameçonnage: 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.

3.2.11 autorité d'enregistrement: acteur de confiance qui établit et/ou se porte garant de l'identité d'une entité devant un fournisseur de services de justificatifs d'identité (CSP).

3.2.12 partie utilisatrice: acteur se fiant à une assertion ou à une déclaration d'identité.

3.2.13 sel: valeur non secrète, souvent aléatoire, qui est employée dans un processus de hachage.

NOTE – On le nomme aussi sable.

3.2.14 secret partagé: secret employé dans l'authentification, qui n'est connu que par l'entité et le contrôleur.

3.2.15 timbre horodateur: paramètre fiable variant dans le temps, qui désigne un point sur l'axe des temps par rapport à une référence commune.

3.2.16 transaction: événement discret faisant intervenir une entité et un fournisseur de services et ayant lieu à des fins commerciales ou à des fins de programmation.

3.2.17 cadre de confiance: ensemble de prescriptions et de mécanismes de mise en application, destiné aux parties qui s'échangent des informations relatives à l'identité.

3.2.18 tierce partie de confiance (TTP, *trusted third party*): autorité ou son agent, auxquels se fient d'autres acteurs, s'agissant d'activités particulières (par exemple, des activités associées à la sécurité).

NOTE – Une tierce partie de confiance est une partie à laquelle se fient une entité et/ou un contrôleur à des fins d'authentification.

3.2.19 période de validité: période dans le temps au cours de laquelle une identité ou un justificatif d'identité peuvent être utilisés lors d'une ou de plusieurs transactions.

3.2.20 contrôle: procédure de confrontation des informations fournies avec des informations précédemment corroborées.

3.2.21 contrôleur: 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.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

CA autorité de certification (*certification authority*)

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

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

EAAF cadre de garantie d'authentification des entités (*entity authentication assurance framework*)

IdM gestion des identités (*identity management*)

IP	protocole Internet (<i>Internet protocol</i>)
LoA	niveau de garantie (<i>level of assurance</i>)
MAC	commande d'accès au support (<i>media access control</i>)
NPE	entité autre qu'une personne (<i>non-person entity</i>)
PDA	assistant numérique personnel (<i>personal digital assistant</i>)
PII	information d'identification personnelle (<i>personally identifiable information</i>)
PIN	numéro d'identification personnel (<i>personal identification number</i>)
RA	autorité d'enregistrement (<i>registration authority</i>)
RP	partie utilisatrice (<i>relying party</i>)
SAML	langage de balisage d'assertion de sécurité (<i>security assertion markup language</i>)
TCP/IP	protocole de commande de transmission/protocole Internet (<i>transmission control protocol/Internet protocol</i>)
TIC	technologie de l'information et de la communication
TLS	sécurité de couche de transport (<i>transport layer security</i>)
TPM	module de plate-forme de confiance (<i>trusted platform module</i>)
TTP	tierce partie de confiance (<i>trusted third party</i>)
URL	identificateur uniforme de ressources (<i>uniform resource locator</i>)

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) "Peut" désigne une autorisation.
- d) "Pourrait" désigne une possibilité ou une capacité.

6 Niveaux de garantie

Le présent cadre de garantie d'authentification des entités (EAAF) définit quatre niveaux de garantie (LoA) pour l'authentification des entités. Chacun des niveaux LoA décrit le degré de confiance dans les processus qui conduisent à la procédure d'authentification et l'intègrent elle-même, offrant ainsi des garanties quant au fait que l'entité qui emploie une identité donnée est bien l'entité à laquelle cette identité a été attribuée. Aux fins de la présente Recommandation, un niveau LoA est une fonction des processus, des activités de gestion et des contrôles techniques qui ont été mis en place par un fournisseur de services de justificatifs d'identité (CSP) pour chacune des phases du cadre EAAF, sur la base de critères établis dans le paragraphe 10. La garantie d'authentification des entités (EAA) est affectée par des considérations de gestion et d'organisation, mais la présente Recommandation ne comporte pas de critère normatif explicite les concernant. Une entité peut être une personne ou une entité autre qu'une personne (NPE).

Cependant, le niveau LoA d'un réseau pourrait être une fonction des niveaux LoA de tous les composants qui forment le réseau et notamment des entités NPE et de tous les dispositifs d'extrémité (par exemple, les téléphones mobiles, les assistants numériques personnels (PDA), les boîtiers décodeurs ou les ordinateurs portables). Dans certains cas, ces dispositifs peuvent se faire passer pour des entités légitimes. En conséquence, la capacité à distinguer avec un certain degré

de confiance un appareil de confiance d'un appareil malveillant est fondamentale pour la garantie EAA.

Le niveau LoA1 est le niveau de garantie le plus bas, tandis que le niveau LoA4 est le niveau de garantie le plus élevé spécifiés dans la présente Recommandation. La détermination du niveau LoA qui convient à une situation donnée dépend de divers facteurs. La définition du niveau LoA requis est essentiellement fondée sur le risque: les conséquences d'une erreur d'authentification et/ou de l'utilisation abusive des justificatifs d'identité, le préjudice et les effets qui en résultent, et la probabilité qu'ils se produisent. Des niveaux LoA plus élevés doivent être employés pour des risques jugés plus grands.

Le cadre EAAF contient des prescriptions et donne des orientations quant à la mise en application, relatives à chacun des quatre niveaux LoA. Il contient en particulier des prescriptions applicables à la mise en oeuvre des procédures, s'agissant des phases suivantes:

- a) Inscription (par exemple, vérification d'identité, contrôle des informations d'identité et enregistrement).
- b) Gestion des justificatifs d'identité (par exemple, délivrance des justificatifs d'identité, activation des justificatifs d'identité).
- c) Authentification.

Il donne aussi des orientations concernant les aspects de gestion et d'organisation (par exemple, la conformité juridique, la gestion de la sécurité des informations) qui influent sur la garantie d'authentification des entités.

Les niveaux LoA sont définis dans le Tableau 6-1 ci-après.

Tableau 6-1 – Niveaux de garantie²

Niveau	Description
1 – Bas	Peu ou pas de confiance dans l'identité déclarée ou affirmée
2 – Moyen	Une certaine confiance dans l'identité déclarée ou affirmée
3 – Elevé	Une grande confiance dans l'identité déclarée ou affirmée
4 – Très élevé	Une très grande confiance dans l'identité déclarée ou affirmée

Ce schéma contient des prescriptions permettant d'atteindre le niveau LoA souhaité pour chacune des phases du cadre de garantie d'authentification des entités. Le niveau LoA global atteint par une mise en oeuvre employant ce cadre sera celui de la phase qui a le niveau LoA le plus bas.

6.1 Niveau de garantie 1 (LoA1)

Au niveau LoA1, la confiance dans l'identité déclarée ou affirmée de l'entité est minimale, mais il existe une certaine confiance dans le fait que l'entité puisse être la même tout au long des événements d'authentification consécutifs. Ce niveau LoA est employé lorsque le risque associé à une authentification erronée est minimal. Aucune prescription particulière n'est donnée concernant le mécanisme d'authentification employé. Il convient seulement qu'il donne une garantie minimale. Une large gamme de technologies disponibles, comprenant des justificatifs d'identité associés aux niveaux LoA plus élevés, peut satisfaire aux prescriptions relatives à la garantie d'authentification

² Le niveau LoA est une fonction des processus, des activités de gestion et des contrôles techniques qui ont été mis en place par un fournisseur CSP pour chacune des phases du cadre EAAF, sur la base des critères établis dans le paragraphe 10.

d'entité pour ce niveau LoA. Ce niveau n'exige pas l'emploi de méthodes d'authentification cryptographique (par exemple, un protocole de demande-réponse utilisant le chiffrement).

Par exemple, le niveau LoA1 peut s'appliquer à une authentification au cours de laquelle une entité présente au site web d'un fournisseur de services un nom d'utilisateur ou un mot de passe qu'elle a enregistré elle-même, pour la création d'une page personnalisée ou pour des transactions impliquant des sites web qui nécessitent un enregistrement en vue d'accéder à des informations ou à de la documentation, telles que des nouvelles ou de la documentation sur des produits.

Au niveau LoA1, une adresse de commande d'accès au support (MAC) peut ainsi satisfaire à une prescription relative à l'authentification d'un appareil. Cependant, il est peu probable qu'un autre appareil ne puisse pas employer la même adresse MAC.

6.2 Niveau de garantie 2 (LoA2)

Au niveau LoA2, il existe une certaine confiance dans l'identité déclarée ou affirmée d'une entité. Ce niveau LoA2 est employé lorsque le risque associé à une authentification erronée est modéré. L'authentification au moyen d'un seul facteur est acceptable. La réussite de l'authentification, au moyen d'un protocole d'authentification sécurisé, doit dépendre de la preuve que donne l'entité qu'elle possède le justificatif d'identité. Des contrôles devraient être mis en place pour réduire l'efficacité des attaques par interception et par conjecture en ligne, mais aussi pour assurer la protection contre les attaques qui visent les justificatifs d'identité archivés.

Par exemple, un fournisseur de services peut exploiter un site web qui permet à ses clients de changer leur adresse consignée. La transaction au cours de laquelle un bénéficiaire change une adresse consignée peut être considérée comme une transaction d'authentification de niveau LoA2, étant donné que cette transaction pourrait comporter un risque modéré de désagrément. Puisque les avis officiels concernant les montants des paiements, l'état des comptes et le rappel des changements sont généralement envoyés à l'adresse consignée du bénéficiaire, la transaction comporte en outre un risque modéré de divulgation non autorisée d'informations PII. En conséquence, le fournisseur de services devrait obtenir au moins une certaine garantie d'authentification avant d'autoriser que la transaction ne se fasse.

6.3 Niveau de garantie 3 (LoA3)

Au niveau LoA3, la confiance dans l'identité déclarée ou affirmée d'une entité est grande. Ce niveau LoA est employé lorsque le risque associé à une authentification erronée est important. Ce niveau LoA doit employer une authentification multifacteur. Toute information secrète échangée dans les protocoles d'authentification doit être protégée par un chiffrement, qu'elle soit en transit ou au repos (même si le niveau LoA3 ne requiert pas l'utilisation d'un protocole de demande-réponse utilisant le chiffrement). Il n'y a pas de prescription concernant la production ou l'archivage des justificatifs d'identité. Ils peuvent être archivés ou produits dans des ordinateurs polyvalents ou dans du matériel spécialisé.

Par exemple, une transaction, au cours de laquelle une société soumet par voie électronique, à un organisme public, certaines informations confidentielles, peut nécessiter une transaction d'authentification de niveau LoA3. Une divulgation induite pourrait entraîner un risque important de perte financière. D'autres exemples de transactions de niveau LoA3 sont notamment l'accès en ligne à des comptes qui permettent à l'entité d'effectuer certaines transactions financières ou l'emploi par un contractant d'une tierce partie d'un système à distance pour accéder à des informations personnelles potentiellement sensibles d'un client.

6.4 Niveau de garantie 4 (LoA4)

Au niveau LoA4, la confiance dans l'identité déclarée ou affirmée d'une entité est très grande. Ce niveau LoA est employé lorsque le risque associé à une authentification erronée est élevé. Le niveau LoA4 fournit le niveau le plus élevé de garantie d'authentification des entités définie par la présente Recommandation. Le niveau LoA4 est semblable au niveau LoA3, mais il exige en plus la vérification en personne des identités des entités qui sont des personnes et l'emploi de dispositifs matériels inviolables pour l'archivage de toutes les clés chiffrées secrètes ou privées. En outre, toutes les informations PII et d'autres données sensibles incorporées dans les protocoles d'authentification doivent être protégées par un chiffrement, qu'elles soient en transit ou au repos.

Par exemple, les services susceptibles de présenter un risque important de dommages ou préjudices en cas d'échec de l'authentification peuvent nécessiter une protection de niveau LoA4. La partie responsable doit bénéficier de la totale garantie que l'entité correcte a fourni certaines informations essentielles, et, si elle omet de vérifier ces informations, elle peut même être jugée pénalement responsable. De même, l'approbation d'une transaction présentant des risques élevés de perte financière peut constituer une transaction de niveau LoA4.

Au niveau LoA4, les certificats numériques (par exemple, les certificats UIT-T X.509 ou les certificats des contrôleurs de cartes (CV)) peuvent être employés pour authentifier les entités NPE, telles que les ordinateurs portables, les téléphones mobiles, les imprimantes, les télécopieurs ou d'autres appareils reliés à un réseau. Ainsi, la procédure d'inscription d'un téléphone intelligent peut nécessiter que soient incorporés dans celui-ci des certificats numériques. Les certificats numériques peuvent également être intégrés aux technologies de mesure intelligentes afin d'empêcher un accès non autorisé au réseau électrique.

6.5 Choix du niveau de garantie approprié

Le choix du niveau LoA approprié devrait être fondé sur une évaluation des risques que présentent les transactions ou les services pour lesquels les entités seront authentifiées. En faisant correspondre les niveaux des incidences aux niveaux LoA, les parties à une transaction d'authentification peuvent déterminer le niveau LoA dont elles ont besoin et peuvent se procurer les services et également se prévaloir d'identités garanties. Le Tableau 6-2 indique les conséquences et les incidences éventuelles d'un échec d'authentification aux divers niveaux LoA.

Tableau 6-2 – Incidences potentielles à chacun des niveaux de garantie

Conséquences éventuelles d'un échec d'authentification	Incidences potentielles d'un échec d'authentification selon les niveaux LoA			
	1	2	3	4
Désagrément, perturbation ou atteinte à la position sociale ou à la réputation	Min*	Mod	Imp	El
Pertes financières ou responsabilité de l'organisme	Min	Mod	Imp	El
Atteinte à l'organisation, à ses programmes ou aux intérêts publics	N/A	Min	Mod	El
Divulgence non autorisée d'informations sensibles	N/A	Mod	Imp	El
Sécurité personnelle	N/A	N.a.	Min Mod	Imp El
Délits civils ou infractions pénales	N/A	Min	Imp	El
* Min = minimales; Mod = modérées; Imp = importantes; El = élevées				

La détermination de ce qu'est un risque minimal, modéré, important ou élevé dépend des critères en matière de risque, établis par l'organisme employant la présente Recommandation pour chacune des conséquences éventuelles. En outre, dans certains cas, plusieurs incidences sont conjuguées (par exemple, les conséquences peuvent inclure une atteinte portée à l'organisation, ainsi qu'une divulgation non autorisée d'informations sensibles). Dans ce type de scénario, il conviendrait d'employer le niveau LoA le plus élevé correspondant aux conséquences.

Chacun des niveaux LoA doit être déterminé par la sévérité et la rigueur des contrôles et des procédures, exécutés au cours de chacune des phases du cadre EAAF par le fournisseur CSP lorsqu'il fournit ses services. Le cadre EAAF impose aux fournisseurs CSP des critères opérationnels en matière de garantie de service à chacun des niveaux LoA. Les critères en matière de garantie de service sont présentés dans le paragraphe 11, des prescriptions plus précises sortant néanmoins du cadre de la présente Recommandation.

Il pourrait y avoir d'autres facteurs associés au commerce dont il conviendrait de tenir compte, au-delà du cadre de la sécurité, lorsque sont utilisés les résultats de l'évaluation des risques pour déterminer le niveau LoA applicable. Ces facteurs commerciaux sont notamment:

- a) la démarche suivie par l'organisme pour gérer les risques résiduels;
- b) le goût d'acceptation du risque par l'organisme, en fonction des incidences indiquées dans le Tableau 6-2;
- c) les objectifs commerciaux pour le service (par exemple, un service dont l'objectif commercial est de favoriser le développement peut être mieux desservi par un niveau LoA plus bas, employant un justificatif d'identité tel qu'un mot de passe, lorsque l'organisme dispose de procédures en vigueur lui permettant de réduire les fraudes et qu'il en accepte le risque avec confiance).

L'évaluation des risques d'une transaction peut se faire dans le cadre d'une évaluation globale des risques en matière de sécurité des informations (notamment, selon la norme ISO/CEI 27001) et devrait être axée sur les besoins spécifiques en matière de sécurité dans les transactions envisagées. Elle doit aborder le risque associé à la garantie d'authentification des entités. Ses résultats doivent être comparés avec ceux pour les quatre niveaux LoA. Le niveau LoA qui correspond le mieux aux résultats de l'évaluation des risques doit être choisi.

Lorsque plusieurs classes de transactions sont envisagées, il est possible qu'un niveau LoA différent s'applique à chacune des transactions ou à chacun des groupes de transactions. En d'autres termes, plusieurs niveaux LoA peuvent être acceptés par un même organisme, en fonction de la transaction particulière considérée.

6.6 Mise en correspondance avec les niveaux LoA et interopérabilité

Selon les domaines, on définira les niveaux LoA différemment. Ces niveaux LoA ne correspondront pas nécessairement de façon biunivoque aux quatre niveaux LoA décrits dans le présent cadre EAAF. Ainsi, dans un domaine, on peut adopter un modèle à quatre niveaux, tandis que, dans un autre domaine, on adoptera un modèle à cinq niveaux. Les différents critères pour les différents modèles d'authentification doivent être définis séparément et être largement diffusés.

Afin d'assurer l'interopérabilité entre les différents modèles de niveaux LoA, il faut expliquer dans chaque domaine comment la mise en correspondance se fait avec les niveaux LoA définis dans la présente Recommandation:

- a) en mettant au point une méthode bien définie de garantie d'authentification des entités, comportant des catégories bien définies de niveaux LoA;
- b) en diffusant largement cette méthode de manière que les organismes souhaitant conclure des accords de type fédératif puissent clairement comprendre les procédures et la terminologie qu'ils emploient mutuellement.

La méthode consistant à employer des niveaux LoA doit en tenir dûment compte et doit les définir clairement en termes d'évaluation des risques, au cours de laquelle sont spécifiés et quantifiés:

- a) les menaces attendues;
- b) les incidences (à savoir, minimales ou modérées) au cas où les menaces deviendraient réalité;
- c) les menaces identifiées devant être contrôlées à chaque niveau LoA;
- d) les technologies et les procédures en matière de sécurité employées lors de l'exécution des contrôles à chacun des niveaux LoA, telles que la spécification d'un justificatif d'identité attribué à un dispositif matériel (par exemple, une carte à puce) ou la spécification des exigences pour la production et l'archivage des justificatifs d'identité;
- e) les critères permettant de déterminer l'équivalence des différentes combinaisons de facteurs d'authentification, en tenant compte de la vérification des identités et des justificatifs d'identité associés.

L'une des démarches, permettant d'aborder la question de la mise en correspondance/concordance des différents modèles à niveaux LoA, peut consister à employer le modèle à quatre niveaux défini dans le présent document et à établir la correspondance avec les autres modèles à n niveaux. Cette méthode permettrait aux fédérations d'identité employant des modèles différents pour la garantie d'authentification d'effectuer la mise en correspondance avec le modèle à quatre niveaux. Les mises en correspondance doivent définir comment les niveaux LoA n'ayant pas de correspondant seront traités, notamment s'ils seront simplement ignorés ou effectivement mis en correspondance avec le niveau qui leur est immédiatement inférieur (puisque qu'il n'y a aucune raison de les faire correspondre à un niveau plus élevé s'il n'y a pas eu de spécification particulière auparavant).

6.7 Echange des résultats d'authentification fondés sur les quatre niveaux LoA

Les acteurs participant à une transaction d'authentification (par exemple, les fournisseurs CSP ou les parties utilisatrices) pourraient avoir à échanger des informations pour mener à bien la transaction ou l'activité.

Les actions consistent notamment, la liste n'étant pas exhaustive:

- a) à permettre à une partie utilisatrice d'exprimer ses attentes en ce qui concerne le niveau LoA auquel l'authentification d'une entité devrait se faire;
- b) à permettre à une entité ou à un fournisseur CSP d'indiquer le niveau LoA réel dans ses réponses;
- c) à permettre à une entité ou à un fournisseur CSP d'annoncer les niveaux LoA pour lesquels sa capacité à satisfaire aux prescriptions associées à ce niveau LoA a été certifiée.

Les acteurs participant à une transaction d'authentification doivent convenir du protocole, de la sémantique, du format et de la structure des informations échangées. La partie utilisatrice devra peut-être spécifier si elle acceptera une réponse en matière d'authentification autre que celle qu'elle avait exactement demandée.

Alors que les certificats numériques sont un moyen bien établi d'acheminer des informations relatives à la garantie des justificatifs d'identité associés, les métadonnées sont de plus en plus utilisées comme moyen de communiquer les obligations en matière de garanties qu'ont les parties s'échangeant des informations. Une "classe de contexte", telle qu'une "classe du contexte d'authentification en langage de balisage d'assertion de sécurité" (SAML) sous la forme d'une adresse URL, est un moyen bien connu, employé par les parties pour communiquer ces classes, s'agissant de la garantie d'authentification dans les demandes et les assertions d'authentification. Par exemple, une assertion type émanant d'un fournisseur d'identité peut acheminer des informations telles que "Cet utilisateur est Jean Dupont, son adresse électronique est jean.dupont@exemple.com, et il a été authentifié dans ce système au moyen d'un mécanisme à mot de passe".

Le reste de ce cadre de garantie porte sur la structure au sein de laquelle les procédures et les prescriptions relatives aux services sont établies, ainsi que sur les menaces et les incidences associées à l'authentification des entités. Pour conclure, il est donné un aperçu de la nécessité de disposer de critères en matière de garantie de service selon lesquels les services peuvent être évalués, de manière à garantir que le niveau LoA adéquat est attribué aux services appropriés de justificatifs d'identité.

7 Acteurs

Les acteurs impliqués dans le cadre EAAF sont notamment les fournisseurs CSP, les autorités d'enregistrement, les parties utilisatrices, les contrôleurs et les tierces parties de confiance. Ces acteurs peuvent appartenir à un seul organisme ou à différents organismes. Il peut y avoir diverses relations et capacités, fournies par un certain nombre d'organismes, notamment des composants, des systèmes et des services partagés ou interagissant entre eux.

7.1 Entité

Une entité a une identité pouvant être authentifiée. Pouvoir authentifier une entité dépend d'un certain nombre de facteurs. Dans le contexte du présent cadre de garantie, cette capacité implique que l'entité a été enregistrée et s'est vue délivrer les justificatifs d'identité appropriés par un fournisseur CSP, un protocole d'authentification ayant été spécifié. Au cours de cette authentification, l'entité peut attester de sa propre identité. Il est aussi possible qu'une autre partie représente l'entité aux fins de l'authentification.

7.2 Fournisseur de services de justificatifs d'identité

Un fournisseur de services de justificatifs d'identité (CSP) délivre et/ou gère des justificatifs d'identité, ou du matériel ou des logiciels et les données associées qui peuvent être employées pour produire des justificatifs d'identité. Les mots de passe et les données biométriques sont des exemples de justificatifs d'identité qui peuvent être délivrés et gérés par un fournisseur CSP. Les cartes à puce contenant des clés privées sont un exemple de matériel et de données associées (pouvant être employées pour produire des justificatifs d'identité), qui peuvent être délivrés et gérés par un fournisseur CSP. Un fournisseur CSP peut aussi délivrer et gérer des données qui peuvent être utilisées pour authentifier des justificatifs d'identité. Si des mots de passe sont employés comme justificatifs d'identité, ces données peuvent être les valeurs des fonctions à sens unique des mots de passe. Si les justificatifs d'identité sont fondés sur des informations signées numériquement, le fournisseur CSP peut produire des certificats de clé publique qui peuvent être employés par les contrôleurs. Les justificatifs d'identité qui sont délivrés et pris en charge ainsi que les moyens de protection, qui sont mis en oeuvre par le fournisseur CSP, sont des facteurs essentiels pour la détermination du niveau LoA qui sera atteint au cours d'une transaction d'authentification donnée (voir également le paragraphe 10.3).

Chaque entité doit se voir délivrer un ou plusieurs justificatifs d'identité ou moyens de les produire, afin qu'une authentification ultérieure puisse se faire. Les justificatifs d'identité ou moyens de les produire ne sont généralement délivrés qu'à l'issue d'une procédure d'inscription réussie, au terme de laquelle l'entité est enregistrée.

7.3 Autorité d'enregistrement

Une autorité d'enregistrement (RA) établit et/ou se porte garante de l'identité d'une entité devant un fournisseur CSP. L'autorité d'enregistrement doit obtenir la confiance du fournisseur CSP pour exécuter les procédures concernant la phase d'inscription et enregistrer les entités d'une manière qui permette au fournisseur CSP d'attribuer ultérieurement des justificatifs d'identité.

Chacune des autorités d'enregistrement doit effectuer un genre de vérification d'identité et de contrôle des informations d'identité selon une procédure spécifiée. Afin de différencier une entité des autres, l'entité se voit généralement attribuer un ou plusieurs identificateurs, qui lui permettront ultérieurement d'être reconnue dans le contexte applicable.

7.4 Partie utilisatrice

Une partie utilisatrice est un acteur tributaire d'une déclaration ou d'une assertion d'identité. Elle peut exiger une identité authentifiée à des fins diverses, telles que la gestion d'un compte, le contrôle d'accès, les décisions en matière d'autorisation, etc. Elle peut effectuer elle-même les opérations nécessaires à l'authentification de l'entité ou elle peut confier ces opérations à une tierce partie.

7.5 Contrôleur

Le contrôleur est un acteur qui corrobore les informations relatives à l'identité. Il peut participer à différentes phases de garantie EAA et peut vérifier les justificatifs d'identité et/ou contrôler les informations d'identité.

7.6 Tierce partie de confiance

Une tierce partie de confiance (TTP) est une autorité ou son agent, qui a la confiance d'autres acteurs en ce qui concerne certaines activités (par exemple, les activités associées à la sécurité). Dans le présent cadre de garantie, une tierce partie TTP a la confiance d'une entité et/ou du contrôleur aux fins de l'authentification. Des exemples de tierces parties aux fins de l'authentification des entités sont notamment les autorités de certification (CA) et les autorités d'horodatage.

8 Phases du cadre de garantie d'authentification des entités

Le présent paragraphe contient un descriptif des phases et des procédures de garantie EAA. Bien que certains modèles EAA puissent différer de la structure du modèle présenté ici, la conformité avec celui-ci exige que les capacités fonctionnelles satisfassent pleinement aux prescriptions décrites dans le présent cadre de garantie. Ce cadre de garantie est technologiquement neutre.

Les organismes adoptant ce cadre de garantie doivent mettre au point des politiques, des procédures et des capacités qui fournissent les méthodes de prise en charge nécessaires et satisfassent aux prescriptions énoncées dans ce cadre de garantie. Celles-ci varieront en fonction du rôle choisi par un organisme particulier et, notamment, en fonction des niveaux LoA auxquels l'organisme délivre les justificatifs d'identité. Ainsi, un organisme peut être soumis:

- a) à des obligations d'actions particulières en son nom ou en celui de ses représentants, concernant des niveaux LoA particuliers;
- b) à des obligations d'évaluation externe ou par une tierce partie d'une de ses capacités opérationnelles dans le cadre EAAF;
- c) à des politiques, à des actions et à des capacités nécessaires pour établir la confiance dans les procédures, les services et les capacités fournies par les organismes adoptant ce cadre de garantie.

8.1 Phase d'inscription

La phase d'inscription comporte quatre procédures: demande et lancement, vérification d'identité, contrôle d'identité et tenue des registres/consignation. Ces procédures peuvent être entièrement exécutées par un seul organisme ou peuvent comporter diverses relations et capacités, fournies par un certain nombre d'organismes, notamment des composants, des systèmes et des services partagés ou interagissant entre eux.

Les procédures requises diffèrent selon la rigueur exigée par le niveau LoA applicable. Dans le cas d'une entité procédant aux inscriptions au niveau LoA1, ces procédures sont minimales (sur une page web, une personne peut notamment appuyer sur un bouton "nouvel utilisateur" et créer un nom d'utilisateur et un mot de passe). Dans d'autres cas, les procédures d'inscription peuvent être plus longues. Ainsi, l'inscription au niveau LoA4 exige une réunion de l'entité et de l'autorité d'enregistrement en personne, ainsi qu'une vérification d'identité approfondie.

8.1.1 Demande et lancement

La phase d'inscription peut débuter de diverses façons. Notamment, elle peut être entamée en réponse à une demande faite par les entités cherchant à obtenir un justificatif d'identité elles-mêmes (par exemple, lorsqu'un nouvel utilisateur d'un site web souhaite obtenir un nom d'utilisateur et un mot de passe). Il est également possible que la procédure d'inscription soit lancée par une tierce partie au nom de l'entité ou par le fournisseur lui-même (s'agissant, par exemple, d'une carte d'identité nationale, d'un badge d'employé). Et puis, à des niveaux LoA élevés, il est possible que les demandes ne soient acceptées que lorsque l'entité est parrainée par une tierce partie.

En tout état de cause, la phase d'inscription des personnes peut débuter en les priant de remplir un formulaire de demande. Ce formulaire doit contenir suffisamment d'informations pour garantir que l'entité puisse être identifiée de manière unique dans un contexte (et doit, par exemple, consigner le nom entier, la date et le lieu de naissance). Pour les entités NPE, telles qu'un appareil mobile, l'inscription peut débuter par l'incorporation de justificatifs d'identité dans l'appareil, qui leur permettent d'être identifiées de manière unique et de recevoir un paramétrage sur mesure par l'intermédiaire d'un profil de configuration chiffré.

Les fournisseurs CSP doivent définir les conditions auxquelles est soumise l'inscription et celles auxquelles est soumise l'utilisation des services associés à cette inscription. Les conditions auxquelles sont soumis les services associés à l'inscription peuvent être établies en conformité avec un cadre de garantie. Selon qu'il convient, les dénis de responsabilité et autres dispositions juridiques doivent être acceptés par l'entité elle-même ou en son nom avant que ne soit poursuivie la procédure d'inscription.

8.1.2 Vérification d'identité et contrôle des informations d'identité

La vérification d'identité est la procédure de collecte et de contrôle d'un nombre suffisant d'informations pour identifier une entité à un niveau de garantie spécifié ou convenu. Le contrôle des informations d'identité est la 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. En fonction du contexte, diverses informations relatives à l'identité (notamment, les cartes nationales d'identité, les permis de conduire, les informations biométriques, les attestations délivrées par des machines, les certificats de naissance) émises ou acceptées par des sources faisant autorité peuvent satisfaire aux obligations en matière de vérification d'identité. Les informations relatives à l'identité concrètement présentées pour satisfaire aux obligations en matière de vérification d'identité varient d'un niveau LoA à l'autre.

La vérification d'identité peut inclure la vérification physique des documents d'identité présentés, en vue de détecter une fraude, une altération ou une contrefaçon éventuelle. Elle peut aussi inclure une vérification devant garantir que l'identité est aussi employée dans d'autres contextes (c'est-à-dire a été contrôlée par d'autres autorités d'enregistrement). Les obligations en matière de vérification d'identité doivent être plus strictes à mesure que le niveau LoA est plus élevé. La procédure de vérification des identités doit aussi être plus stricte pour les entités affirmant ou déclarant une identité à distance (notamment, par l'intermédiaire d'un canal en ligne) que pour celles qui le font localement (par exemple, en personne auprès d'une autorité d'enregistrement).

La rigueur des obligations en matière de vérification d'identité est fondée sur les objectifs qui doivent être atteints pour chaque niveau LoA. Au niveau LoA1, le seul objectif consiste à garantir que l'identité est unique dans le contexte considéré. L'identité ne devrait pas être associée à deux entités différentes. Au niveau LoA2, les objectifs sont au nombre de deux. En premier lieu, l'identité doit être unique dans le contexte. En deuxième lieu, l'entité à laquelle se rapporte l'identité doit exister objectivement, ce qui veut dire que l'identité n'est pas fictive ou intentionnellement fabriquée à des fins frauduleuses³. Ainsi, la vérification de l'identité des personnes au niveau LoA2 peut inclure la confrontation avec les registres des naissances et des décès afin de garantir une certaine provenance (même si cela ne prouve pas que l'entité en possession d'un certificat de naissance est l'entité à laquelle ce certificat se rapporte). De même, la vérification de l'identité des entités NPE au niveau LoA2 peut inclure la vérification d'un numéro de série auprès du fabricant.

Au niveau LoA3, les objectifs sont ceux des niveaux LoA1 et LoA2, ainsi que l'objectif qui consiste à contrôler les informations relatives à l'identité auprès d'une ou de plusieurs sources faisant autorité, telles qu'une base de données externe. Le contrôle des informations d'identité montre que l'identité est en usage et se rapporte à l'entité. Toutefois, rien ne garantit que les informations relatives à l'identité sont en la possession du détenteur réel et légitime de l'identité. Pour les personnes, au niveau LoA4, il est ajouté un objectif à ceux du niveau LoA3, exigeant que les entités soient reconnues en personne afin d'éviter l'usurpation.

Les procédures de vérification des identités à un niveau LoA donné doivent inclure les procédures des niveaux inférieurs. Par exemple, la vérification d'identité au niveau LoA3 suppose qu'il a été satisfait aux contrôles de vérification des identités aux niveaux LoA1 et LoA2.

Tableau 8-1 – Application des objectifs de vérification d'identité aux niveaux LoA

Niveau LoA	Description	Objectif	Contrôles	Méthode appliquée⁴
Niveau LoA1 – bas	Peu ou pas de confiance dans l'identité déclarée ou affirmée	L'identité est unique dans un contexte	Autodéclaration ou auto-affirmation	Localement ou à distance
Niveau LoA2 – moyen	Une certaine confiance dans l'identité déclarée ou affirmée	L'identité est unique dans un contexte et l'entité à laquelle elle se rapporte existe objectivement	Preuve de l'identité au moyen d'informations relatives à l'identité provenant d'une source faisant autorité	Localement ou à distance
Niveau LoA3 – élevé	Une grande confiance dans l'identité déclarée ou affirmée	L'identité est unique dans un contexte, l'entité à laquelle elle se rapporte existe objectivement, l'identité est contrôlée et l'identité est utilisée dans d'autres contextes	Preuve de l'identité au moyen d'informations relatives à l'identité provenant d'une source faisant autorité + contrôle des informations d'identité	Localement ou à distance

³ Cela n'exclut pas l'emploi de pseudonymes.

⁴ La vérification d'identité à distance se fait par l'intermédiaire d'un réseau et implique que l'entité ne peut être observée physiquement tandis que la vérification d'identité localement se fait d'une manière qui exige de voir l'entité physiquement.

Tableau 8-1 – Application des objectifs de vérification d'identité aux niveaux LoA

Niveau LoA	Description	Objectif	Contrôles	Méthode appliquée ⁴
Niveau LoA4 – très élevé	Une très grande confiance dans l'identité déclarée ou affirmée	L'identité est unique dans un contexte, l'entité à laquelle elle se rapporte existe objectivement, l'identité est contrôlée et l'identité est utilisée dans d'autres contextes	Preuve de l'identité au moyen d'informations relatives à l'identité provenant de plusieurs sources faisant autorité + contrôle des informations d'identité + entité reconnue en personne ⁵	Localement seulement

Les contrôles requis aux niveaux LoA pour assurer la protection contre les menaces lors de l'inscription doivent être déterminés par l'emploi des contrôles énumérés dans le paragraphe 10.1.2.

Toute mise en oeuvre du cadre EAAF repose sur tout (ou partie) des informations relatives à l'identité et sur les sources qui sont à la disposition des entités potentielles et/ou de l'autorité d'enregistrement.

La fiabilité et l'exactitude de ces justificatifs d'identité, des informations relatives à l'identité et des sources définissent la garantie réelle qu'offre la phase d'inscription. En conséquence, les responsables de la mise en oeuvre du cadre EAAF doivent examiner avec soin la garantie, fournie par les infrastructures (de gestion) des identités qui sont employées par les différentes sources et entités émettrices, lorsqu'ils décident des justificatifs d'identité, des informations relatives à l'identité et/ou des sources qui sont fiables à des fins de vérification d'identité et de contrôle des informations d'identité. Toute mise en oeuvre du cadre EAAF doit inclure la publication d'un document (par exemple, concernant la politique de contrôle des identités, décrite dans le paragraphe 10.1.2.1) qui donne un aperçu des informations relatives à l'identité, des sources et/ou des entités émettrices fiables, venant à l'appui au cours de la phase d'inscription.

8.1.3 Tenue des registres/consignation

Il s'agit de la procédure d'achèvement de l'inscription d'une entité. La procédure de tenue des registres, au cours de la phase d'inscription, consiste à créer une rubrique faisant état de l'inscription. Cette rubrique doit contenir les informations et la documentation qui ont été recueillies (et peuvent être gardées), les informations concernant la procédure de contrôle des informations d'identité, les résultats de ces étapes et toute autre donnée pertinente. Une décision est alors rendue et consignée, en vue d'accepter ou de refuser l'inscription ou de la reporter pour examen ultérieur ou autre suite à donner.

8.1.4 Enregistrement

L'enregistrement est une procédure au cours de laquelle une entité demande d'employer un service ou une ressource. Bien que la procédure d'enregistrement soit généralement considérée comme faisant partie de la procédure d'inscription, de sorte qu'elle est exécutée à la fin de la phase d'inscription, elle peut également être exécutée ultérieurement. A la différence d'autres procédures au cours de l'inscription qui ne doivent probablement être exécutée qu'une seule fois, l'enregistrement peut être nécessaire lorsqu'une entité demande pour la première fois un accès à un service ou à une ressource donnés.

⁵ Le contrôle de la reconnaissance en personne ne s'applique qu'aux entités qui sont des personnes.

8.2 Phase de gestion des justificatifs d'identité

La phase de gestion des justificatifs d'identité comporte toutes les procédures se rapportant à la gestion de la durée de vie d'un justificatif d'identité ou du moyen de le produire, afin que l'utilisateur puisse participer à une activité ou à un environnement. La phase de gestion des justificatifs d'identité peut comporter tout ou partie des procédures suivantes: l'établissement des justificatifs d'identité, la délivrance des justificatifs d'identité ou des moyens de les produire, l'activation des justificatifs d'identité ou des moyens de les produire, l'archivage des justificatifs d'identité, la révocation et/ou la destruction des justificatifs d'identité ou des moyens de les produire, le renouvellement et/ou le remplacement des justificatifs d'identité ou des moyens de les produire et la tenue des registres. Certaines de ces procédures dépendent de la question de savoir si le justificatif d'identité est intégré dans un dispositif matériel.

8.2.1 Etablissement des justificatifs d'identité

La procédure d'établissement des justificatifs d'identité englobe tous les processus nécessaires pour établir un justificatif d'identité, ou un moyen de le produire, pour la première fois. Ces processus peuvent inclure le prétraitement, l'initialisation et le lien.

8.2.1.1 Prétraitement des justificatifs d'identité

Certains justificatifs d'identité ou moyens de les produire nécessitent un prétraitement avant la délivrance, tel qu'une personnalisation lorsque le justificatif d'identité est adapté à l'identité de l'entité. Une personnalisation peut prendre différentes formes, en fonction du justificatif d'identité. Ainsi, la personnalisation d'une carte à puce qui contient des justificatifs d'identité peut impliquer l'impression (sur une face de la carte) ou l'écriture (sur la puce de la carte) du nom de l'entité à laquelle la carte sera délivrée. Il existe aussi des justificatifs d'identité qui ne nécessitent aucune personnalisation, tels que les mots de passe.

8.2.1.2 Initialisation des justificatifs d'identité

L'initialisation des justificatifs d'identité englobe toutes les étapes visant à garantir qu'un moyen de produire un justificatif d'identité sera ultérieurement en mesure d'assurer les fonctionnalités dont on s'attend qu'il les assure. Par exemple, il se pourrait qu'une carte à puce doive calculer les paires de clés chiffrées, nécessaires à une prise en charge ultérieure de la production de signatures numériques. De même, une carte à puce pourrait être délivrée dans un état "verrouillé", nécessitant l'introduction d'un numéro PIN au cours de la procédure d'activation.

8.2.1.3 Lien des justificatifs d'identité

Le lien est la procédure d'association d'un justificatif d'identité, ou du moyen de le produire, à une entité à laquelle il sera délivré. La manière dont ce lien est établi et la confiance dans le lien dépend du niveau LoA. Ainsi, dans un scénario en ligne, lorsque le pseudonyme identificateur habituel d'une entité est lié à la fiche client d'une entité, un premier "code d'activation" peut être acheminé au cours de la procédure d'établissement du lien, par un canal sécurisé, dans un mouchard chiffré applicable à la session seulement. A l'inverse, le code d'activation peut être demandé à la fin de la procédure, une fois l'étape de lien de l'entité à l'identificateur habituel achevée, afin de lier l'identificateur habituel à la fiche client.

8.2.2 Délivrance des justificatifs d'identité

La délivrance des justificatifs d'identité est la procédure qui consiste à fournir à une entité un justificatif d'identité ou un moyen de le produire particulier ou à associer l'entité à celui-ci. La complexité de cette procédure est fonction du niveau LoA requis. Pour des niveaux LoA élevés, il sera nécessaire de fournir en toute sécurité un dispositif matériel (par exemple, une carte à puce) contenant un justificatif d'identité et il se pourrait que ce dispositif doive être fourni en personne. Dans le cas de niveaux LoA plus bas, la procédure de délivrance pourrait simplement consister en l'envoi d'un mot de passe ou d'un numéro PIN à l'adresse physique ou électronique de l'entité.

Pour les entités NPE, telles que des appareils, les procédures de délivrance aux niveaux LoA supérieurs débutent généralement lorsque le fabricant de l'appareil commande des certificats numériques en vrac, communiquant pour ce faire au fournisseur CSP une liste des numéros uniques d'identification des appareils pour chacun des certificats numériques. Le fournisseur CSP, en guise de réponse, lui fournit des certificats et des clés privées sous une forme chiffrée. Au cours du processus de fabrication, le fabricant peut incorporer un certificat numérique dans chacun des appareils, lui attribuant ainsi un identificateur unique.

8.2.3 Activation des justificatifs d'identité

L'activation des justificatifs d'identité est la procédure au moyen de laquelle un justificatif d'identité ou le moyen de le produire est rendu prêt à l'emploi. La procédure d'activation peut comporter diverses mesures, selon le justificatif d'identité. Ainsi, un justificatif d'identité, ou le moyen de le produire, peut avoir été "verrouillé" après son initialisation, afin de prévenir une utilisation abusive, jusqu'au moment de la délivrance à l'entité. Dans ces cas, l'activation peut consister à "déverrouiller" le justificatif d'identité (par exemple, au moyen d'un mot de passe). Un justificatif d'identité ou le moyen de le produire peut aussi être réactivé après une suspension au cours de laquelle sa validité a été temporairement interrompue.

8.2.4 Archivage des justificatifs d'identité

L'archivage des justificatifs d'identité est la procédure au cours de laquelle les justificatifs d'identité ou les moyens de les produire sont archivés en lieu sûr d'une manière qui les protège contre toute divulgation, utilisation, modification ou destruction non autorisée. Il implique tant l'entité associée à un justificatif d'identité que les actions requises pour éviter l'utilisation non autorisée d'un justificatif d'identité.

Cependant, il n'implique pas nécessairement la protection des informations employées pour vérifier qu'un justificatif d'identité est légitime, si ces informations ne font pas partie du justificatif d'identité. La protection des informations, telles que des tableaux de mots de passe hachés nécessaires pour l'authentification, est exigée à des niveaux LoA élevés.

8.2.5 Suspension, révocation et/ou destruction des justificatifs d'identité

La révocation est la procédure au cours de laquelle il est définitivement mis fin à la validité d'un justificatif d'identité. La suspension est une procédure qui y est liée, au cours de laquelle la validité d'un justificatif d'identité est temporairement interrompue. La révocation peut s'appliquer dans de nombreux cas différents, tels que les cas suivants:

- a) Un justificatif d'identité ou un moyen de le produire a été signalé comme ayant été perdu, volé ou autrement compromis.
- b) Un justificatif d'identité a expiré.
- c) La possession d'un justificatif d'identité ne se justifie plus (par exemple, lorsqu'un employé quitte son employeur).
- d) Un justificatif d'identité a été utilisé à des fins non autorisées.
- e) Un justificatif d'identité différent a été délivré en remplacement du justificatif d'identité en question.

Le laps de temps entre l'observation d'un événement exigeant la révocation et l'achèvement de la procédure de révocation dépend de la politique en matière d'organisation. Aux niveaux LoA plus élevés, le laps de temps admis avant la révocation est généralement plus court. Certains justificatifs d'identité, tels que ceux qui figurent sur les cartes à puce, peuvent être physiquement détruits à la suite d'une révocation. Mais les informations associées au justificatif d'identité ne peuvent pas toujours être détruites.

8.2.6 Renouvellement et/ou remplacement des justificatifs d'identité

Le renouvellement est la procédure au cours de laquelle la durée de vie d'un justificatif d'identité existant est prolongée. Le remplacement est la procédure au cours de laquelle une entité se voit délivrer un nouveau justificatif d'identité ou un moyen de le produire, pour remplacer un justificatif d'identité précédemment délivré qui a été révoqué. Un justificatif d'identité de remplacement est, par exemple, employé lorsqu'un fournisseur CSP envoie un mot de passe temporaire à l'adresse électronique d'une entité, qui permet à celle-ci de créer un nouveau mot de passe après avoir fourni le mot de passe temporaire. Un autre exemple est un code de déverrouillage de numéro PIN, que l'on devrait traiter comme un numéro PIN. La rigueur des procédures de renouvellement et de remplacement des justificatifs d'identité dépend des niveaux LoA.

8.2.7 Tenue des registres

Des rubriques appropriées doivent être tenues à jour tout au long de la durée de vie d'un justificatif d'identité. Elles doivent au moins signaler:

- a) le fait qu'un justificatif d'identité a été établi;
- b) l'identificateur du justificatif d'identité (le cas échéant);
- c) l'entité à laquelle le justificatif d'identité a été délivré (le cas échéant);
- d) le statut du justificatif d'identité (le cas échéant).

Des registres doivent être tenus pour toutes les procédures (applicables) associées à la phase de gestion des justificatifs d'identité. Lorsque des justificatifs d'identité sont délivrés à des personnes, la tenue des registres est susceptible d'impliquer le traitement d'informations PII (voir l'Appendice I).

8.3 Phase d'authentification des entités

Au cours de la phase d'authentification des entités, l'entité emploie son justificatif d'identité pour attester de son identité auprès d'une partie utilisatrice. La procédure d'authentification consiste seulement à établir (ou pas) la confiance dans la déclaration ou l'assertion d'identité, et elle n'a aucune incidence sur les actions que la partie utilisatrice peut vouloir mener en se fondant sur la déclaration ou l'assertion. Elle n'a en outre aucun rapport avec lesdites actions.

8.3.1 Authentification

Afin d'établir la confiance dans une identité, la procédure d'authentification utilise un protocole, permettant de démontrer la possession d'un justificatif d'identité, et/ou de contrôler ledit justificatif d'identité. Les prescriptions du protocole d'authentification sont fonction du niveau LoA applicable. Par exemple, à un bas niveau LoA, l'authentification peut impliquer l'emploi d'un mot de passe. A des niveaux LoA plus élevés, l'authentification peut impliquer l'emploi d'un protocole de demande-réponse utilisant le chiffrement. L'authentification multifacteur est exigée aux niveaux LoA plus élevés. Les facteurs d'authentification n'ont pas tous la même rigueur et plusieurs facteurs sont employés pour renforcer la garantie (voir le paragraphe 10).

8.3.2 Tenue des registres

Le suivi et la tenue des registres des événements au cours de la phase d'authentification peuvent être nécessaires à des fins diverses, telles que le respect des obligations en matière de fourniture de service, de conformité, de responsabilité et/ou les obligations juridiques.

Lorsque des personnes sont concernées, les informations contenues dans ces rubriques peuvent comporter des informations sensibles. Ces rubriques doivent être gérées de manière à prendre en compte le besoin de protection et de minimisation des informations PII (voir aussi l'Appendice I).

9 Considérations de gestion et d'organisation

La garantie EAA ne dépend pas uniquement des facteurs techniques mais aussi des règlements, des accords contractuels et des considérations sur la manière dont la fourniture des services est dirigée et organisée. Une solution rigoureuse sur le plan technique, sans gestion ni exploitation compétentes, peut ne pas être en mesure de fournir de manière sûre la garantie EAA.

Le présent paragraphe est informatif et contient des considérations d'organisation et de gestion qui touchent la garantie EAA. Il ne fournit pas de critères spécifiques pour chaque niveau LoA. Les critères spécifiques et l'évaluation de la conformité en ce qui concerne les aspects de gestion et d'organisation sortent du cadre de la présente Recommandation mais devraient être incorporés dans un cadre de garantie.

9.1 Etablissement du service

L'établissement du service concerne tant le statut juridique du fournisseur de services que la fourniture du service sur le plan fonctionnel. Ainsi, savoir que le fournisseur des services de gestion et d'authentification des identités est une entité juridique enregistrée donne confiance dans le fait que le fournisseur CSP est une entreprise loyale dans la juridiction dans laquelle il opère. Cette question est plus importante lorsque les composantes de service sont exploitées par différentes entités juridiques (par exemple, l'enregistrement en tant que fonction distincte).

Bien que les prescriptions fondamentales soient les mêmes pour tous les niveaux LoA, les niveaux plus élevés devraient dépendre plus de la question de savoir si la fourniture du service est complète et fiable. Par exemple, au niveau LoA3 et plus haut, une plus grande confiance dans la fourniture du service devrait aussi découler de la connaissance de ses liens avec les sociétés et de la compréhension du niveau d'indépendance autorisé dans son fonctionnement.

9.2 Conformité juridique et contractuelle

Tous les acteurs du cadre EAAF devraient comprendre les obligations juridiques qui leur incombent en rapport avec l'exploitation et la fourniture du service et s'y conformer. Cela a des incidences notamment, mais pas uniquement, sur les types d'informations qui peuvent être recherchées, sur la manière dont la vérification des identités est effectuée et sur les informations qui peuvent être retenues. Le traitement des informations PII constitue un problème juridique particulier (voir l'Appendice I). Il conviendrait de tenir compte de toutes les juridictions dans lesquelles les acteurs opèrent. A partir du niveau LoA2, il conviendrait de définir les prescriptions en matière de politique et les prescriptions contractuelles spécifiques.

9.3 Dispositions financières

Lorsqu'une disponibilité des services à long terme est envisagée tant par une entité que par les parties utilisatrices, la stabilité financière devrait s'avérer suffisante pour assurer l'exploitation continue du service et pour prendre en charge le degré de responsabilité encouru. Les services et la fiabilité au niveau LoA1 ne devraient que très peu faire intervenir ces considérations, alors que les services assurant des transactions plus importantes à partir du niveau LoA2 devraient satisfaire à ces besoins.

9.4 Gestion de la sécurité des informations et audit

A partir du niveau LoA2, les acteurs du cadre EAAF devraient établir des pratiques motivées en matière de gestion de la sécurité des informations, des politiques, des approches en matière de gestion des risques et d'autres contrôles reconnus, de manière à garantir que les méthodes en place sont efficaces. A partir du niveau LoA3, un système officiel de gestion de la sécurité des informations (voir par exemple [b-ISO/CEI 27000]) devrait être employé.

En fonction des accords concernant la conformité juridique, contractuelle et technique, les acteurs devraient faire en sorte que les parties respectent leurs engagements et puissent offrir une voie de recours dans l'éventualité où ce ne serait pas le cas. A partir du niveau LoA2, cette garantie doit être renforcée par des audits sur la sécurité, tant internes qu'externes, et un archivage sûr des événements importants, notamment concernant ces audits. Un audit peut servir à vérifier que les pratiques des parties sont conformes à celles dont il a été convenu. Les services de règlement des différends peuvent intervenir en cas de désaccord.

9.5 Composantes extérieures de service

Lorsqu'un organisme dépend de tierces parties pour certains de ses services, la manière dont il dirige les actions de ces parties et surveille celles-ci influera sur la garantie globale de la fourniture du service. La nature et la portée de ces arrangements devraient dépendre du niveau LoA requis et du système de gestion de la sécurité des informations employé. Au niveau LoA1, cette garantie devrait avoir un effet minimal, mais à partir du niveau LoA2 ces mesures contribuent à la garantie globale fournie.

9.6 Infrastructure opérationnelle

Afin de disposer d'un réseau de confiance à grande échelle, on peut instaurer un cadre de confiance. Dans un cadre de confiance, les acteurs se chargent d'acheminer les informations entre eux. En fonction des accords, des acteurs supplémentaires peuvent intervenir afin de garantir que tous les acteurs respectent leurs engagements et puissent offrir une voie de recours si tel n'était pas le cas.

9.7 Capacités opérationnelles d'évaluation

Les décideurs énoncent les prescriptions techniques et contractuelles applicables aux cadres de confiance. Les prescriptions techniques pourraient, par exemple, inclure la version des produits, la configuration des systèmes, les réglages et les protocoles, alors que les prescriptions contractuelles pourraient être axées sur les pratiques équitables en matière d'information. Tandis qu'ils établissent ces prescriptions, les décideurs devraient inclure des critères permettant d'évaluer les entités susceptibles d'évoluer dans un cadre de confiance. Cependant, plutôt que de définir eux-mêmes ces critères, ils voudront peut-être se fonder sur des critères normalisés déjà définis par des experts, tels que ceux qui sont énoncés dans la présente Recommandation. Plus les décideurs utiliseront des critères normalisés dans les différents cadres de confiance, plus il sera facile pour les entités de comprendre ces critères et de les appliquer de manière cohérente. En outre, l'attribution d'un nom aux ensembles de critères peut servir à indiquer de manière abrégée les différents degrés ou types de rigueur des prescriptions ou des capacités aux divers niveaux LoA.

10 Menaces et contrôles

Ce paragraphe décrit les menaces pour chacune des phases du cadre EAAF et présente les contrôles requis à chaque niveau LoA.

10.1 Menaces pour la phase d'inscription et contrôles applicables

10.1.1 Menaces pour la phase d'inscription

Le Tableau 10-1 répertorie et décrit les menaces pour la phase d'inscription.

Tableau 10-1 – Menaces pour la phase d'inscription

Menace	Exemples
Impersonation	A titre d'exemples d'usurpation, on peut citer celui d'une entité qui utilise illégalement des informations relatives à l'identité d'une autre entité et celui d'un dispositif qui s'enregistre auprès d'un réseau en employant une adresse fictive de commande d'accès au support (MAC).

10.1.2 Contrôles requis aux niveaux LoA pour la protection de la phase d'inscription contre les menaces

Le Tableau 10-2 répertorie les contrôles requis pour la phase d'inscription, selon les niveaux LoA.

Tableau 10-2 – Contrôles au cours de la phase d'inscription pour chacun des niveaux LoA

Menace	Contrôles	Contrôles requis			
		LoA1	LoA2	LoA3	LoA4
Impersonation	IdentityProofing: PolicyAdherence	#1	#1	#1	#1
	IdentityProofing: In Person	/	/	/	#2
	IdentityProofing: AuthoritativeInformation	#3	#4	#5	#6

NOTE – Dans le tableau ci-dessus, les identificateurs #1 à #6 correspondent aux contrôles spécifiques requis pour assurer la protection à chacun des niveaux LoA. Chacun de ces contrôles est décrit en détails dans le paragraphe 10.1.2.1. Lorsque les cases du tableau contiennent une ligne en diagonale, cela veut dire que le contrôle en question ne s'applique pas au niveau LoA indiqué.

10.1.2.1 Contrôles contre les menaces pour la phase d'inscription

Les contrôles suivants contre les menaces pour la phase d'inscription correspondent aux identificateurs #1 à #6 énumérés dans le Tableau 10-2.

IdentityProofing: PolicyAdherence

#1. Publier la politique de vérification des identités et effectuer la vérification de toutes les identités conformément à ladite politique.

IdentityProofing: In Person

#2. La vérification en personne des identités doit être employée pour les personnes.

IdentityProofing: AuthoritativeInformation

#3. Les informations relatives à l'identité peuvent être autodéclarées ou auto-affirmées.

#4. Les contrôles suivants s'appliquent:

- Tous les contrôles du #3.
- En outre:
- L'entité doit fournir des informations d'identité provenant d'au moins une source faisant autorité, conforme à la politique.
 - a) Pour les personnes:
 - i) En personne:
 - Garantir que l'entité est en possession d'un document d'identification, provenant d'au moins une source faisant autorité, conforme à la politique, et présentant une photographie ressemblante du détenteur.
 - Garantir que le document d'identification présenté est un document authentique, délivré dans les règles et valable au moment de la demande.

ii) Pas en personne:

- L'entité doit prouver qu'elle est en possession d'informations d'identité personnelles, conformes à la politique (des informations d'identité acceptables sont, par exemple, un permis de conduire ou un passeport).
- L'existence et la validité de la preuve fournie doivent être confirmées conformément aux prescriptions en matière de politique.

b) Pour les entités NPE:

- Informations archivées provenant d'une source faisant autorité d'informations d'identité, telles que le nom usuel, la description, le numéro de série, l'adresse MAC, le propriétaire, l'emplacement, le fabricant, etc.

#5. Les contrôles suivants s'appliquent:

- Tous les contrôles du #4.

En outre:

a) Pour les personnes:

i) En personne:

- Contrôler l'exactitude des informations de contact énumérées dans le document d'identification en les utilisant pour contacter l'entité.
- Contrôler au moins un document d'identification (par exemple, un document attestant de la naissance, du mariage ou de l'immigration) en le comparant aux registres de la source pertinente faisant autorité.
- Corroborer les informations personnelles auprès de sources pertinentes faisant autorité et (si possible) auprès de sources d'autres contextes à même de garantir qu'il n'y a aucune ambiguïté quant à l'identité.
- Contrôler les informations précédemment fournies par l'entité ou susceptibles d'être connues d'elle seule.

ii) Pas en personne:

- Garantir l'examen, par une tierce partie de confiance, de l'assertion/de la déclaration de l'entité, selon laquelle celle-ci est en possession d'un justificatif d'identité de niveau LoA3 (ou supérieur) provenant d'une source faisant autorité.
- Contrôler les informations précédemment fournies par l'entité ou susceptibles d'être connues d'elle seule.

b) Pour les entités NPE:

- Du matériel de confiance (par exemple, un module TPM) doit être employé au niveau LoA3.
- S'agissant des entités NPE déjà en service, elles doivent être physiquement inscrites auprès d'une entité d'enregistrement au moyen d'un justificatif d'identité de niveau LoA3 délivré par une personne. Lorsque du matériel de confiance est employé, il devrait être activé.
- Les entités NPE non encore disponibles doivent être commandées au moyen de l'authentification ou des signatures numériques de niveau LoA3 d'une personne afin qu'il soit confirmé que l'entité effectuant la commande est autorisée à commander l'entité NPE. L'autorité d'enregistrement du fabricant doit enregistrer l'entité NPE, activer tout matériel de confiance et contrôler la délivrance et la personnalisation de l'entité NPE. Le matériel de confiance doit être initialisé à l'aide d'une connexion au réseau.

- Pour les entités NPE autres que les ordinateurs, le lien entre le dispositif, le propriétaire, l'exploitant du réseau ou de la communication et l'autorité d'enregistrement doit être sécurisé par un chiffrement d'une manière semblable à celle qui est appliquée à un ordinateur de confiance.
- Lorsqu'un logiciel est employé, le code doit être signé numériquement avant la délivrance, à l'aide d'un justificatif d'identité de niveau LoA3 délivré par une personne, et doit être contresigné par l'autorité d'enregistrement comme preuve d'acceptation avant sa mise en service.

#6. Les contrôles suivants s'appliquent:

- Tous les contrôles du #5.

En outre:

a) Pour les personnes:

- L'entité doit fournir des informations d'identité provenant d'au moins une autre source faisant autorité, conforme à la politique.

b) Pour les entités NPE:

- Les dispositifs supplémentaires reliés à un ordinateur, à un téléphone intelligent ou à un processeur analogue doivent être consignés lors de la délivrance et attachés par un chiffrement au dispositif d'ancrage (par exemple, un dispositif de confiance activé matériellement, un lecteur biométrique, des cartes à puce, le géo-authentificateur GPS).
- Toute modification des arrangements concernant les liens entre les dispositifs doit être gérée par l'intermédiaire de l'autorité d'enregistrement. Si possible, la capacité de gestion du réseau devrait alerter l'autorité d'enregistrement ou la gestion du réseau de tout changement dans les relations entre les dispositifs et des éventuelles mesures correctrices prises.
- Une capacité doit être mise en place pour empêcher le fonctionnement de toute relation altérée entre les dispositifs.
- Le code d'un logiciel de niveau LoA4 doit être signé numériquement, à l'aide d'un justificatif d'identité de niveau LoA4 délivré par une personne, et doit être contresigné par l'autorité d'enregistrement comme preuve d'acceptation avant sa mise en service.

10.2 Menaces pour la phase de gestion des justificatifs d'identité et contrôles applicables

10.2.1 Menaces pour la gestion des justificatifs d'identité

Le Tableau 10-3 énumère les menaces pour la phase de gestion des justificatifs d'identité.

Tableau 10-3 – Menaces pour la gestion des justificatifs d'identité

Menaces	Exemples
CredentialCreation: Tampering	Un attaquant altère des informations alors que celles-ci passent de la procédure d'inscription à la procédure de création du justificatif d'identité.
CredentialCreation: UnauthorizedCreation	Un attaquant entraîne le fournisseur CSP à créer un justificatif d'identité fondé sur une entité fictive.
CredentialIssuance: Disclosure	Un justificatif d'identité créé par le fournisseur CSP pour une entité est copié par un attaquant alors qu'il est transporté du fournisseur CSP jusqu'à l'entité au cours de l'établissement du justificatif d'identité.
CredentialActivation: Unauthorized Possession	Un attaquant obtient un justificatif d'identité qui ne lui appartient pas et, usurpant l'identité de l'entité légitime, entraîne le fournisseur CSP à activer le justificatif d'identité.
CredentialActivation: Unavailability	<ol style="list-style-type: none"> 1) L'entité associée à un justificatif d'identité ou moyen de le produire n'est pas à l'emplacement habituel et n'est pas en mesure d'authentifier comme il convient son identité auprès du fournisseur CSP. 2) La délivrance d'un justificatif d'identité ou du moyen de produire ce justificatif est retardée et l'activation dans le délai prescrit n'est pas possible.
CredentialStorage: Disclosure	Les justificatifs d'identité archivés dans un fichier du système sont divulgués. Par exemple, un attaquant accède au fichier dans lequel les noms d'utilisateur et les mots de passe sont archivés.
CredentialStorage: Tampering	Le fichier où est établie la correspondance entre les noms d'utilisateur et les justificatifs d'identité est compromis de manière que les correspondances sont modifiées et que les justificatifs d'identité existants sont remplacés par des justificatifs d'identité auxquels l'attaquant a accès.
CredentialStorage: Duplication	Un attaquant emploie des informations archivées pour créer le double d'un justificatif d'identité (par exemple, en reproduisant une carte à puce susceptible de produire le justificatif d'identité), qui peut être employé par une entité non autorisée.
CredentialStorage: DisclosureByEntity	L'entité conserve par écrit le nom d'utilisateur et le mot de passe, en un lieu accessible à d'autres.
CredentialRevocation: DelayedRevocation	Les informations de révocation ne sont pas diffusées à temps, d'où la menace que des entités dont les justificatifs ont été révoqués puissent encore s'authentifier avant que le contrôleur ne mette à jour ses informations de révocation.
CredentialRevocation: UseAfterDecommissioning	<p>Les comptes utilisateur ne sont pas supprimés lorsque les employés quittent une entreprise, d'où la possibilité d'une utilisation abusive des anciens comptes par des personnes non autorisées.</p> <ul style="list-style-type: none"> – Un justificatif d'identité intégré dans un dispositif matériel est employé après la révocation de ses clés chiffrées.
CredentialRenewal: Disclosure	Le justificatif renouvelé par le fournisseur CSP pour une entité est copié par un attaquant lors de son transport.
CredentialRenewal: Tampering	Un nouveau justificatif créé par une entité est modifié par un attaquant lors de sa soumission au fournisseur CSP en vue de remplacer le justificatif expiré.

Tableau 10-3 – Menaces pour la gestion des justificatifs d'identité

Menaces	Exemples
CredentialRenewal: UnauthorizedRenewal	Un attaquant est en mesure de tirer profit d'un protocole peu rigoureux de renouvellement des justificatifs d'identité dans le but de prolonger la période de validité d'un justificatif d'identité pour une entité. Un attaquant induit le fournisseur CSP en erreur et le pousse à délivrer un nouveau justificatif d'identité pour une entité, le nouveau justificatif d'identité liant l'identité de l'entité au justificatif d'identité fourni par l'attaquant. Pour les entités NPE, on peut citer à titre d'exemple le réétiquetage (la redélivrance) d'un composant de système (par exemple, la mémoire RAM) comme étant neuf alors qu'il a déjà été employé.
CredentialRecordkeeping: Repudiation	Une entité affirme ou déclare qu'un justificatif d'identité légitime est frauduleux ou contient des informations incorrectes en vue de nier faussement avoir utilisé le justificatif d'identité.

10.2.2 Contrôles requis aux niveaux LoA pour la protection de la phase de gestion des justificatifs d'identité contre les menaces

Le Tableau 10-4 répertorie les contrôles requis, selon le niveau LoA, contre les menaces pour la gestion des justificatifs d'identité.

Tableau 10-4 – Contrôles lors de la gestion des justificatifs d'identité pour chacun des niveaux LoA

Menaces	Contrôles	Contrôles requis			
		LoA1	LoA2	LoA3	LoA4
CredentialCreation: Tampering	AppropriateCredentialCreation	#1	#1	#2	#2
	HardwareOnly				#3
	StateLocked				#4
CredentialCreation: UnauthorizedCreation	TrackedInventory	#5	#5	#5	#5
CredentialIssuance: Disclosure	AppropriateCredentialIssuance	#6	#7	#7	#8
CredentialActivation: UnauthorizedPossession CredentialActivation: Unavailability	ActivatedByEntity	#9	#9	#10	#11
CredentialStorage: Disclosure CredentialStorage: Tampering CredentialStorage: Duplication CredentialStorage: DisclosureByEntity	CredentialSecureStorage	#12	#13	#14	#15
CredentialRevocation: DelayedRevocation CredentialRevocation: UseAfterDecommissioning	CredentialSecureRevocation &Destruction	#16	#16	#16	#16
CredentialRenewal: Disclosure CredentialRenewal: Tampering CredentialRenewal: UnauthorizedRenewal	CredentialSecureRenewal	#17	#17	#18	#19
CredentialRecordkeeping: Repudiation	RecordRetention	#20	#20	#21	#21

NOTE – Dans le tableau ci-dessus, les identificateurs #1 à #21 correspondent aux contrôles spécifiques requis pour assurer la protection à chacun des niveaux LoA. Chacun de ces contrôles est décrit en détails dans le paragraphe 10.2.2.1. Lorsque les cases du tableau contiennent une ligne en diagonale, cela veut dire que le contrôle en question ne s'applique pas au niveau LoA indiqué.

10.2.2.1 Contrôles contre les menaces pour la phase de gestion des justificatifs d'identité

Les contrôles suivants contre les menaces pour la phase de gestion des justificatifs d'identité correspondent aux identificateurs # 1 à # 21 énumérés dans le Tableau 10-4.

AppropriateCredentialCreation

#1. Les contrôles suivants s'appliquent:

- Des procédures officielles et étayées doivent être employées pour la création des justificatifs d'identité.
- Avant de lier définitivement un justificatif à une entité, le fournisseur CSP doit s'être bien assuré que ce justificatif est et reste lié à la bonne entité.

#2. Les contrôles suivants s'appliquent:

- Tous les contrôles du #1.

En outre:

- Le lien des justificatifs d'identité doit assurer une protection contre l'altération en employant:
 - a) soit des signatures numériques;
 - b) soit les mécanismes décrits dans le contrôle StateLocked pour les justificatifs d'identité intégrés dans un dispositif matériel.

HardwareOnly

#3. Les justificatifs d'identité doivent être intégrés dans un module matériel de sécurité⁶.

StateLocked

#4. Les justificatifs d'identité intégrés dans un module matériel de sécurité doivent être placés dans un état verrouillé à la fin de la procédure de création.

TrackedInventory

#5. Lorsqu'un justificatif d'identité ou le moyen de le produire est intégré dans un dispositif matériel, celui-ci doit être physiquement en sécurité et l'inventaire doit être suivi de près. Ainsi, des cartes à puce non personnalisées devraient être entreposées dans un lieu sûr et leurs numéros de série archivés afin d'assurer la protection contre le vol et les tentatives par la suite de créer des justificatifs d'identité non autorisés.

AppropriateCredentialIssuance

#6. Des procédures officielles et étayées doivent être employées pour la délivrance des justificatifs d'identité.

#7. Les contrôles suivants s'appliquent:

- Tous les contrôles du #6.

⁶ La frontière d'un module matériel de sécurité est définie dans la norme ISO/CEI 19790:2012.

En outre:

- La procédure de délivrance doit inclure un mécanisme permettant de garantir qu'un justificatif d'identité est fourni à l'entité correcte ou à un représentant autorisé. Si le justificatif d'identité n'est pas fourni à une personne, un mécanisme doit être utilisé pour contrôler que l'adresse de livraison existe et est légitimement associée à l'entité.

#8. Les contrôles suivants s'appliquent:

- Tous les contrôles du #7.

En outre:

- Si le justificatif d'identité n'est pas fourni à une personne, sa fourniture doit se faire par une voie sécurisée et l'entité ou un représentant autorisé de l'entité doit signer un accusé de réception du justificatif d'identité.

ActivatedByEntity

#9. Une procédure doit exister visant à garantir qu'un justificatif d'identité, ou le moyen de le produire, n'est activé que s'il est sous le contrôle de l'entité prévue. Il n'y a aucune prescription spécifique concernant cette procédure.

#10. Une procédure doit exister visant à garantir qu'un justificatif d'identité, ou le moyen de le produire, n'est activé que s'il est sous le contrôle de l'entité prévue. Cette procédure doit prouver que l'entité est liée à l'activation d'un justificatif d'identité (par exemple un protocole de demande-réponse).

#11. Une procédure doit exister visant à garantir qu'un justificatif d'identité, ou le moyen de le produire, n'est activé que s'il est sous le contrôle de l'entité prévue. Cette procédure:

- a) doit prouver que l'entité est liée à l'activation d'un justificatif d'identité (par exemple un protocole de demande-réponse);
- b) ne doit autoriser l'activation que pendant une durée déterminée par la politique.

CredentialSecureStorage

#12. Les contrôles suivants s'appliquent:

- Les justificatifs d'identité fondés sur des secrets partagés doivent être protégés par des contrôles d'accès qui limitent l'accès aux seuls administrateurs et applications qui nécessitent un accès.
- La politique de protection des justificatifs d'identité archivés doit être décrite dans la documentation, relative à l'emploi de ces justificatifs d'identité, qui est mise à la disposition des entités.

#13. Les contrôles suivants s'appliquent:

- Tous les contrôles du #12.

En outre:

- Ces fichiers secrets partagés ne doivent pas contenir de mots de passe ou de secrets en clair. Une autre méthode peut être employée pour protéger le secret partagé.

#14. Les contrôles suivants s'appliquent:

- Tous les contrôles du #13.

En outre:

- Les secrets partagés doivent être protégés par des contrôles d'accès qui limitent l'accès aux seuls administrateurs et applications qui nécessitent un accès. Ces secrets partagés doivent être chiffrés. La clé de chiffrement pour le secret partagé doit elle-même être chiffrée et archivée dans un module chiffré (matériel ou logiciel). La clé de chiffrement pour le secret

partagé ne doit être déchiffrée que si elle est, immédiatement après, requise pour une opération d'authentification.

- Les entités ou les représentants autorisés des entités sont tenus de déclarer qu'ils comprennent ces prescriptions et acceptent de protéger les justificatifs d'identité conformément à ces prescriptions.

#15. Les contrôles suivants s'appliquent:

- Tous les contrôles du #14.

En outre:

- Les entités ou les représentants autorisés des entités sont tenus de signer un document déclarant qu'ils comprennent les prescriptions applicables à l'archivage des justificatifs d'identité et acceptent de protéger ceux-ci en conséquence.

CredentialSecureRevocation&Destruction

#16. Les fournisseurs CSP doivent révoquer ou détruire (si possible) les justificatifs d'identité (notamment ceux qui sont fondés sur des secrets partagés) dans un délai propre à chaque niveau LoA, comme défini par la politique en matière d'organisation.

CredentialSecureRenewal

#17. Les contrôles suivants s'appliquent:

- Le fournisseur CSP doit établir des politiques appropriées pour le renouvellement et le remplacement des justificatifs d'identité.
- La preuve de la possession d'un justificatif d'identité en cours de validité doit être démontrée par l'entité avant que le fournisseur CSP n'autorise le renouvellement et/ou le remplacement.
- Les mots de passe doivent satisfaire aux prescriptions minimales en matière de politique du fournisseur CSP, applicables à la solidité et au réemploi des mots de passe.
- Après expiration du justificatif d'identité en cours de validité, le renouvellement ne doit pas être autorisé.
- Toutes les interactions doivent se faire par une voie protégée.

#18. Les contrôles suivants s'appliquent:

- Tous les contrôles du #17.

En outre:

- Une vérification d'identité au niveau LoA2 sera effectuée conformément au paragraphe 10.1.2.1 (IdentityProofing: PolicyAdherence, IdentityProofing: AuthoritativeInformation).

#19. Les contrôles suivants s'appliquent:

- Tous les contrôles du #17.

En outre:

- Une vérification d'identité au niveau LoA3 sera effectuée conformément au paragraphe 10.1.2.1 (IdentityProofing: PolicyAdherence, IdentityProofing: AuthoritativeInformation).

RecordRetention

#20. L'enregistrement, l'historique et le statut de chaque justificatif d'identité (notamment la révocation) doivent être consignés par le fournisseur CSP. La durée de conservation doit être spécifiée dans la politique du fournisseur CSP.

#21. Les contrôles suivants s'appliquent:

- Tous les contrôles du #20.
- Des procédures officielles et étayées doivent être élaborées concernant la filière de conservation de chaque consignment.

10.3 Menaces pour la phase d'authentification et contrôles applicables

10.3.1 Menaces pour la phase d'authentification

Les menaces pour la phase d'authentification sont tant les menaces associées à l'emploi des justificatifs d'identité lors de l'authentification que les menaces générales pour l'authentification. Les menaces générales pour l'authentification sont notamment, mais la liste n'est pas exhaustive: les logiciels malveillants (par exemple, les virus, les chevaux de Troie, les enregistreurs de frappe de clavier), l'ingénierie sociale (par exemple, la lecture par-dessus l'épaule, le vol de dispositifs matériels et de numéros PIN), les erreurs des utilisateurs (par exemple, les mots de passe peu solides, la mauvaise protection des informations d'identification), la fausse répudiation, l'interception et/ou la modification non autorisées des données d'authentification au cours de la transmission, le déni de service et les faiblesses procédurales. Mis à part l'emploi de l'authentification multifacteur, les contrôles contre les menaces générales pour l'authentification sortent du cadre de la présente Recommandation. Le présent paragraphe se concentre sur les menaces associées à l'utilisation des justificatifs d'identité employés pour l'authentification. Il décrit ces menaces et répertorie les contrôles applicables à chaque type de menace.

Sauf en ce qui concerne l'obligation d'employer l'authentification multifacteur pour les niveaux LoA3 et LoA4, il ne convient pas de délimiter les contrôles spécifiques en termes de niveau LoA pour la phase d'authentification. Certains contrôles peuvent ne pas convenir à tous les contextes. Ainsi, les contrôles applicables à l'authentification des utilisateurs accédant aux abonnements à des journaux en ligne sont probablement différents de ceux qui sont appliqués par les médecins pour accéder aux dossiers de leurs patients. Il est donc recommandé, puisque les risques et les conséquences d'une exploitation s'amplifient de plus en plus, que le fournisseur CSP examine en profondeur, la question de la sécurité (à savoir en établissant une hiérarchie des contrôles en fonction de l'environnement opérationnel, de l'application et du niveau LoA). Il incombe au concepteur du système de prendre, sur la base d'une analyse des risques, les décisions concernant la question de savoir comment, quand et dans quel ordre procéder à ces contrôles.

Les menaces pour les justificatifs d'identité lors de l'authentification sont nombreuses. Le Tableau 10-5 énumère les grandes catégories de menaces pour l'utilisation des justificatifs d'identité et donne des exemples spécifiques illustrant ces menaces.

Tableau 10-5 – Résumé des menaces pour l'utilisation des justificatifs d'identité au cours de la phase d'authentification

Menaces	Exemples
Menaces générales	Les menaces générales pour l'authentification se répartissent entre de nombreuses catégories communes à tout type de TIC. A titre d'exemple, on peut citer les enregistreurs de frappe de clavier, l'ingénierie sociale et les erreurs des utilisateurs. Mis à part l'emploi de l'authentification multifacteur, les contrôles contre ces menaces sortent du cadre de la présente Recommandation. Il est à noter que l'authentification multifacteur n'assure pas une protection contre toutes les menaces générales possibles.
OnlineGuessing	Un attaquant tente de façon répétée d'ouvrir une session en devinant des valeurs possibles du justificatif d'identité.
OfflineGuessing	<p>Les secrets associés à la génération de justificatifs d'identité sont dévoilés au moyen de méthodes analytiques en dehors de la transaction d'authentification. Le perçage des mots de passe repose souvent sur des méthodes employant la force, telles que l'emploi d'attaques par dictionnaire. Dans ce cas, un attaquant emploie un programme pour passer en revue, par itération, tous les mots d'un dictionnaire (ou de plusieurs dictionnaires de langues différentes), calcule la valeur hachée de chacun des mots et confronte cette valeur hachée avec la base de données.</p> <p>L'emploi des tables arc-en-ciel est une autre méthode de perçage des mots de passe. Les tables arc-en-ciel sont des tables calculées d'avance de paires texte clair/valeur hachée. Elles permettent d'être plus rapide que les attaques en force parce qu'elles emploient des fonctions permettant de réduire l'espace de recherche. Une fois produites ou obtenues, les tables arc-en-ciel peuvent être utilisées de manière répétée par un attaquant.</p>
CredentialDuplication	Le justificatif d'identité d'une entité ou le moyen de le produire a été illégalement copié. A titre d'exemple, on peut citer la copie non autorisée d'une clé privée.
Phishing	Une entité est incitée à interagir avec un faux contrôleur et frauduleusement conduite à révéler son mot de passe ou des données personnelles sensibles qui peuvent être employées pour se substituer à elle. C'est le cas, par exemple, lorsqu'une entité se voit envoyer un message électronique la redirigeant vers un site web frauduleux et demandant à l'utilisateur d'ouvrir une session en employant son nom d'utilisateur et son mot de passe.
Eavesdropping	Un attaquant écoute passivement la transaction d'authentification pour recueillir des informations qui peuvent être employées, lors d'une attaque active ultérieure, pour se substituer à l'entité.
ReplayAttack	Un attaquant est en mesure de réutiliser des messages (entre une entité légitime et une partie utilisatrice) précédemment capturés pour s'authentifier à la place de ladite entité auprès de la partie utilisatrice.
SessionHijack	Un attaquant est en mesure de s'introduire lui-même entre une entité et un contrôleur à la suite d'un échange d'authentification réussi entre ces deux parties. Il est en mesure de se faire passer pour une entité auprès de la partie utilisatrice ou inversement de prendre la commande de l'échange des données au cours de la session. A titre d'exemple, on peut citer le cas d'un attaquant qui est en mesure de reprendre une session déjà authentifiée, à l'aide de la valeur, obtenue par écoute ou prévision, des mouchards d'authentification, employés pour marquer les demandes HTTP envoyées par l'entité.

Tableau 10-5 – Résumé des menaces pour l'utilisation des justificatifs d'identité au cours de la phase d'authentification

Menaces	Exemples
ManInTheMiddle	L'attaquant se positionne entre l'entité et la partie utilisatrice de manière à pouvoir intercepter et altérer le contenu des messages du protocole d'authentification. L'attaquant usurpe généralement l'identité de l'entité aux yeux du contrôleur. Le fait d'avoir un échange actif avec les deux parties simultanément peut lui permettre d'employer les messages d'authentification que l'une des parties légitimes envoie pour pouvoir s'authentifier auprès de l'autre.
CredentialTheft	Un dispositif qui produit ou contient des justificatifs d'identité est volé par un attaquant.
SpoofingAndMasquerading	La simulation et l'usurpation renvoient à des situations dans lesquelles un attaquant usurpe l'identité d'une autre entité afin de pouvoir exécuter une action qu'il n'aurait sinon pas été en mesure d'exécuter (par exemple, en vue d'accéder à des ressources autrement inaccessibles). Cela peut être fait en employant un ou plusieurs justificatifs d'identité d'une entité ou sinon en se substituant à l'entité (par exemple, en créant un justificatif d'identité). A titre d'exemples, on peut citer le cas d'un attaquant usurpant l'identité d'une entité, qui simule une ou plusieurs caractéristiques biométriques en créant une configuration "malléable" qui concorde avec celle de l'entité, le cas d'un attaquant usurpant une adresse MAC en faisant en sorte que son dispositif diffuse une adresse MAC qui appartient à un autre dispositif, disposant de permissions sur un réseau particulier, ou le cas d'un attaquant qui se substitue à un responsable légitime d'un éditeur de logiciels pour télécharger en ligne des applications et/ou des mises à jour logicielles.

10.3.2 Contrôles requis aux niveaux LoA, visant à protéger l'utilisation des justificatifs d'identité contre les menaces

Le Tableau 10-6 répertorie les contrôles requis pour lutter contre les menaces pour l'utilisation des justificatifs d'identité, selon les niveaux LoA.

Tableau 10-6 – Résumé des contrôles contre les menaces pour l'utilisation des justificatifs d'identité, selon les niveaux LoA

Menaces	Contrôles	Contrôles requis				
		LoA*	LoA1	LoA2	LoA3	LoA4
Menaces générales**	MultiFactorAuthentication				#1	#1
OnlineGuessing	StrongPassword CredentialLockOut DefaultAccountUse AuditAndAnalyze	#2 #3 #4 #5				
OfflineGuessing	HashedPasswordWithSalt	#6				
CredentialDuplication	AntiCounterfeiting	#7				
Phishing	DetectPhishingFromMessages AdoptAntiPhishingPractice MutualAuthentication	#8 #9 #10				
Eavesdropping	NoTransmitPassword	#11				

Tableau 10-6 – Résumé des contrôles contre les menaces pour l'utilisation des justificatifs d'identité, selon les niveaux LoA

Menaces	Contrôles	Contrôles requis				
		LoA*	LoA1	LoA2	LoA3	LoA4
	EncryptedAuthentication	#12	/	/	/	/
	DifferentAuthenticationParameter	#13	/	/	/	/
ReplayAttack	DifferentAuthenticationParameter	#13	/	/	/	/
	Timestamp	#14	/	/	/	/
	PhysicalSecurity	#15	/	/	/	/
SessionHijacking	EncryptedSession	#16	/	/	/	/
	FixProtocolVulnerabilities	#17	/	/	/	/
	CryptographicMutualHandshake	#18	/	/	/	/
ManInTheMiddle	MutualAuthentication	#10	/	/	/	/
	EncryptedSession	#16	/	/	/	/
CredentialTheft	CredentialActivation	#19	/	/	/	/
SpoofingAndMasquerading	CodeDigitalSignature	#20	/	/	/	/
	LivenessDetection	#21	/	/	/	/
LoA* – Ces contrôles devraient s'appliquer si l'évaluation des risques le juge nécessaire. Menaces générales** – L'authentification multifacteur ne permet pas de contrer toutes les menaces générales.						

NOTE – Dans le tableau ci-dessus, les identificateurs #1 à #21 correspondent aux contrôles spécifiques requis pour assurer la protection à chacun des niveaux LoA. Chacun de ces contrôles est décrit en détails dans le paragraphe 10.3.2.1

10.3.2.1 Contrôles contre les menaces pour l'utilisation des justificatifs d'identité au cours de la phase d'authentification

Les contrôles suivants contre les menaces pour l'utilisation d'un justificatif d'identité au cours de la phase d'authentification correspondent aux identificateurs #1 à #21 énumérés dans le Tableau 10-6.

MultiFactorAuthentication

#1. Deux ou plusieurs justificatifs d'identité s'appuyant sur différents facteurs d'authentification doivent être employés (par exemple, une chose que vous combinez avec une chose que vous connaissez).

StrongPassword

#2. L'emploi de mots de passe solides (par exemple, des mots de passe complexes, des chaînes de caractères ne figurant pas dans un dictionnaire et mélangeant les caractères majuscules, minuscules, numériques et spéciaux) doit être respecté.

CredentialLockout

#3. Un mécanisme de verrouillage ou de ralentissement doit être employé après qu'un certain nombre de tentatives de saisie de mot de passe ont échoué.

DefaultAccountUse

#4. Des noms et des mots de passe d'utilisateur par défaut (par exemple, les réglages du fabricant) ne doivent pas être employés.

AuditAndAnalyze

#5. Un journal d'audit des échecs de connexion doit être employé pour analyser les caractéristiques de tentatives visant à deviner les mots de passe en ligne.

HashedPasswordWithSalt

#6. Les mots de passe hachés saupoudrés de sel doivent être employés pour lutter contre les attaques employant la force ou s'appuyant sur des tables arc-en-ciel.

Anticounterfeiting

#7. Des mesures anticontrefaçon (par exemple, les hologrammes, les impressions microscopiques) doivent être employées sur les dispositifs contenant des justificatifs d'identité.

DetectPhishingFromMessages

#8. Des contrôles doivent être mis en oeuvre, qui soient spécialement conçus pour détecter les attaques par hameçonnage (par exemple, des filtres bayésiens, des liste noires IP, des filtres fondés sur les adresses URL, des schémas heuristiques et à empreintes digitales).

AdoptAntiPhishingPractice

#9. Des pratiques, telles que la désactivation des images, la désactivation des liens hypertextes avec des sources non fiables et la fourniture de signaux visuels aux clients de la messagerie électronique, doivent être employées pour protéger les entités contre les attaques par hameçonnage.

MutualAuthentication

#10. L'authentification mutuelle doit être employée.

NoTransmitPassword

#11. Des mécanismes d'authentification qui ne transmettent pas les mots de passe sur le réseau doivent être employés (par exemple, le protocole Kerberos).

EncryptedAuthentication

#12. Si un échange d'authentification sur un réseau est nécessaire, les données doivent être chiffrées avant le transit.

DifferentAuthenticationParameter

#13. Un paramètre d'authentification différent doit être employé pour chaque transaction d'authentification (par exemple, un mot de passe ou un justificatif d'identité de session, à usage unique).

Timestamp

#14. Chacun des messages doit être horodaté à l'aide d'un timbre horodateur non falsifiable.

PhysicalSecurity

#15. Des mécanismes physiques de sécurité doivent être employés (par exemple, la preuve d'une altération, sa détection et la réponse qui y est donnée).

EncryptedSession

#16. Des sessions chiffrées doivent être employées.

FixProtocolVulnerabilities

#17. Des programmes de correction au niveau des plates-formes doivent être employés pour déterminer les vulnérabilités du protocole (par exemple, TCP/IP).

CryptographicMutualHandshake

#18. Un échange mutuel de prise de contact fondé sur le chiffrement (par exemple, TLS) doit être employé.

CredentialActivation

#19. L'emploi d'un justificatif d'identité doit être soumis à une activation (par exemple, au moyen de l'introduction d'un numéro PIN ou d'informations biométriques dans le dispositif matériel contenant le justificatif d'identité).

CodeDigitalSignature

#20. Les signatures numériques doivent être contrôlées auprès d'une source de confiance pour lutter contre le téléchargement de logiciels qui ont été modifiés par des parties non autorisées à le faire.

LivenessDetection

#21. Des techniques de détection du caractère vivant doivent être employées pour repérer l'utilisation de caractéristiques biométriques artificielles (par exemple, des empreintes digitales falsifiées).

11 Critères de garantie de service

Dans un cadre de confiance, les opérateurs qui cherchent à se conformer à ce cadre de garantie doivent établir des critères spécifiques satisfaisant aux prescriptions de chacun des niveaux LoA qu'ils envisagent de prendre en charge et doivent évaluer, selon ces critères, les fournisseurs CSP qui affirment se conformer au cadre de garantie. De même, les fournisseurs CSP doivent déterminer le niveau LoA de ce cadre de garantie, auquel se conforment leurs services, en évaluant globalement, selon des critères spécifiques, leurs procédures commerciales et leurs mécanismes techniques.

Annexe A

Caractéristiques d'un justificatif d'identité

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

- a) Un justificatif d'identité est un ensemble de données.
- Un justificatif d'identité n'inclut aucun conteneur ni dispositif physique qui contient les données. Il n'inclut pas non plus le générateur qui crée les données constituant le justificatif d'identité. Donc, le générateur de codes de passe ne fait jamais partie d'un justificatif d'identité, ni la carte à puce qui peut signer des données, ni le logiciel qui produit des signatures numériques ou le papier sur lequel des choses pourraient être écrites.
- b) Un justificatif d'identité doit contenir des données qui sont une preuve de l'identité et/ou de l'habilitation.
- Des exemples de preuve sont les suivants:
- 1) une chose connue (par exemple, un mot de passe statique);
 - 2) une caractéristique biométrique ou une représentation de celle-ci;
 - 3) des données produites par une chose possédée (par exemple, des codes de passe à usage unique produits par un générateur de codes de passe, des données qui sont numériquement signées par un matériel ou un logiciel employant une clé privée, supposée être la possession d'une entité).
- c) Un justificatif d'identité peut être accompagné d'autres données qui peuvent être utiles pour les procédures d'authentification et d'identification, sans faire partie du justificatif d'identité proprement dit.
- Des exemples de telles données sont notamment le nom d'une entité ou un certificat de clé publique. Aucune de ces informations n'est nécessaire comme preuve d'identité ou d'habilitation, mais elles sont utiles dans les protocoles d'authentification. Associer le nom de l'entité à un justificatif d'identité confirme l'identité. Associer un certificat de clé publique à un justificatif d'identité donne non seulement des informations qui étayent la preuve mais aussi éventuellement des informations sur l'identité ou l'habilitation d'une entité.
- d) Un justificatif peut également être un justificatif dérivé.
- Dans ce cas, un tel justificatif dérivé peut être un ensemble d'informations provenant d'un ensemble de justificatifs, généralement créé et envoyé par une entité en vue d'une authentification auprès d'un contrôleur de justificatifs. Par exemple, pour certaines authentifications anonymes, l'entité transforme le justificatif délivré par le fournisseur CSP en justificatif dérivé qui est utilisé aux fins de son authentification.
- e) Les données comprenant un justificatif d'identité ne doivent pas toutes être tenues secrètes.
- f) Un justificatif d'identité peut être employé pour l'authentification, l'identification ou l'autorisation de l'entité, ou pour une combinaison des trois.
- g) Un justificatif d'identité doit être contrôlé avant de pouvoir être accepté comme authentique et fiable dans un but particulier (par exemple, l'authentification, l'identification, l'autorisation).
- h) Le contrôle d'un justificatif d'identité doit se faire en plusieurs étapes. Des exemples de telles étapes sont notamment:
- 1) La vérification de l'authenticité du justificatif d'identité en vue de garantir qu'il a été délivré par le prétendu émetteur.

- 2) La confirmation de la validité et de la fiabilité du justificatif d'identité, par exemple, en déterminant s'il existe un lien direct avec une racine de confiance de l'émetteur du justificatif d'identité.
 - 3) La confirmation de l'exactitude du calcul mathématique/chiffré.
- i) Un justificatif d'identité peut être authentique mais non valable dans tous les contextes (par exemple, le justificatif d'identité sur une carte à puce, telle qu'une carte téléphonique prépayée, peut être authentique, mais seulement valable pour les appels passant par les installations de l'émetteur).

Appendice I

Confidentialité et protection des informations d'identification personnelle

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

Le fait pour une méthode particulière d'authentification d'être adaptée à un usage particulier dépendra non seulement de l'évaluation de l'efficacité de l'authentification mais aussi de celle des risques et de la tolérance aux risques des organismes impliqués. La mauvaise utilisation ou l'absence d'une protection appropriée des informations PII des entités conduisent à des risques importants pour les organismes, allant de l'atteinte à leur réputation à un engagement de leur responsabilité. L'emploi des informations PII à des fins d'authentification et leur protection doivent en conséquence être soigneusement soupesés et examinés. Le présent Appendice donne des orientations, à titre informatif, en ce qui concerne certains aspects de la confidentialité, dont les organismes devraient tenir compte lorsqu'ils décident d'employer une méthode d'authentification particulière et de la mettre en oeuvre.

Lorsque les entités sont des personnes, la plupart des méthodes d'authentification nécessiteront un traitement des informations PII au cours d'une ou de plusieurs des étapes suivantes:

- a) au cours de la procédure d'inscription, lors de la collecte, de la vérification et du contrôle de l'identité et d'autres informations relatives aux entités;
- b) au cours de la création, de la délivrance et de la gestion des justificatifs d'identité des entités;
- c) au cours de l'emploi des justificatifs d'identité par l'entité et de leur contrôle par les parties utilisatrices et par les contrôleurs.

Il est possible d'assurer une authentification stricte et une confidentialité stricte. Il existe de nombreuses méthodes d'authentification, strictes en matière de chiffrement, qui n'ont qu'un faible impact négatif sur la vie privée (par exemple, les justificatifs d'identité anonymes, les signatures en groupe). En outre, il convient de noter que le relèvement du niveau de garantie (par exemple, du niveau LoA2 au niveau LoA4) peut, mais pas nécessairement, porter atteinte à la vie privée d'une personne. Cela dépendra pour beaucoup de la méthode d'authentification choisie et de la manière dont elle est appliquée. En prenant ces décisions, chaque organisme devrait envisager avec soin la nécessité de protéger les informations PII des entités, outre la nécessité de protéger leurs ressources et de rendre lesdites entités responsables en cas d'activités non autorisées.

La plupart des méthodes d'authentification font appel à l'utilisation d'identifiants distinctifs pour distinguer de façon non ambiguë une entité des autres entités possibles dans le contexte d'une authentification. L'emploi des identifiants distinctifs est souvent aussi nécessaire à d'autres fins, telles que la gestion des comptes et l'établissement d'un journal d'audit approprié. Les principales préoccupations en matière de confidentialité, se rapportant à l'emploi d'identifiants distinctifs, ne concernent pas l'usage d'un identifiant distinctif en tant que tel, mais plutôt le réemploi du même identifiant dans de nombreuses configurations différentes. Ainsi, un numéro de compte attribué dans un but unique est généralement considéré comme étant moins sensible qu'une référence publique administrative employée à des fins multiples (par exemple, les impôts, les soins de santé, la retraite). Dans certaines juridictions, il peut aussi exister une législation restreignant l'usage de certains identifiants.

En raison de ce qui précède, les organismes devraient appliquer des mesures efficaces de protection des informations PII des entités au cours des phases et des procédures décrites dans ce cadre EAAF. En particulier, la méthode d'authentification choisie devrait être conçue et appliquée d'une manière qui, de façon générale, minimise le traitement des informations PII. En outre, l'emploi d'identifiants distinctifs, qui sont aussi utilisés dans d'autres contextes ou domaines, devrait se

limiter aux cas où il est nécessaire de les employer et où les lois de la ou des juridictions pertinentes le permettent.

Des orientations supplémentaires formulées par l'ISO/CEI concernant la protection des informations PII sont données dans les deux références suivantes:

- a) [b-ISO/CEI 29100] contient des prescriptions de base en matière de confidentialité, qui s'articulent autour de trois grands thèmes: 1) les prescriptions juridiques et réglementaires visant à protéger la vie privée des personnes et leurs informations PII; 2) les prescriptions particulières liées aux échanges commerciaux et aux cas d'utilisation; et 3) les préférences individuelles en matière de confidentialité de l'entité détentrice des informations PII. [b-ISO/CEI 29100] décrit les principes de base suivants en matière de confidentialité: consentement et choix, spécification de l'objectif, restrictions en matière de collecte, utilisation, restrictions en matière de rétention et de divulgation, minimisation des données, ouverture à l'égard de l'exactitude et de la qualité, transparence et annonce, participation et accès individuels, comptabilité, contrôles de sécurité et conformité. Outre qu'ils devraient procéder à une évaluation des risques en vue d'analyser les menaces, les organismes devraient procéder à une évaluation de l'incidence de leur méthode d'authentification sur la confidentialité, afin de déterminer quels composants de leurs systèmes ont besoin d'une attention particulière en termes de mesures de protection de la vie privée.
- b) [b-ISO/CEI 29101] présente un cadre architectural pour les systèmes TIC traitant des informations PII. Les objectifs de ce cadre et plusieurs points de vue architecturaux sont présentés. Un ensemble de composants est défini pour la mise en oeuvre des systèmes TIC traitant des informations PII. Le cadre présenté doit servir à la construction d'architectures de système répondant aux principes de confidentialité énoncés dans [b-ISO/CEI 29100].

Pour des orientations détaillées en matière de prescriptions, de principes et de conception des systèmes, s'agissant de la protection des informations PII, le lecteur est prié de se reporter aux normes susmentionnées.

Bibliographie

- [b-UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité.*
- [b-UIT-T Y.2702] Recommandation UIT-T Y.2702 (2008), *Spécifications d'authentification et d'autorisation dans les réseaux de prochaine génération de version 1.*
- [b-UIT-T Y.2720] Recommandation UIT-T Y.2720 (2009), *Cadre de gestion d'identité des réseaux NGN.*
- [b-UIT-T Y.2721] Recommandation UIT-T Y.2721 (2010), *Spécifications et cas d'utilisation de la gestion d'identité dans les réseaux NGN.*
- [b-UIT-T Y.2722] Recommandation UIT-T Y.2722 (2011), *Mécanismes de gestion d'identité dans les réseaux de prochaine génération.*
- [b-ISO/CEI 9798] ISO/CEI 9798:2010, *Technologies de l'information – Techniques de sécurité – Authentification d'entité.*
- [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 19792] ISO/CEI 19792:2009, *Technologies de l'information – Techniques de sécurité – Cadre de la sécurité pour l'évaluation et le test de la technologie biométrique.*
- [b-ISO/CEI 27000] ISO/CEI 27000:2012, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire.*
- [b-ISO/CEI 27001] ISO/CEI 27001:2005, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences.*
- [b-ISO/CEI 29100] ISO/CEI 29100:2011, *Technologies de l'information – Techniques de sécurité – Cadre privé.*
- [b-ISO/CEI 29101] ISO/CEI 29101, *Technologies de l'information – Techniques de sécurité – Architecture de référence de la protection de la vie privée.*
- [b-ISO/CEI 24760-1] ISO/CEI 24760-1:2011, *Technologies de l'information – Techniques de sécurité – Cadre pour la gestion de l'identité – Partie 1: Terminologie et concepts.*
- [b-NIST SP800-36] NIST Special Pub 800-36 (2003), *Guide to Selecting Information Technology Security Products.*
<<http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf>>
- [b-NIST SP800-63] NIST Special Pub 800-63 (2006), *Electronic Authentication Guideline Version 1.0.2.*
<http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>
- [b-AGGPKI] *Australian Government Gatekeeper Public Key Infrastructure.*
<http://www.gatekeeper.gov.au/>

- [b-DuD] Van Alsenoy B. et De Cock, D. (2008), *Due processing of personal data in eGovernment? A Case Study of the Belgian electronic identity card*, *Datenschutz und Datensicherheit*, Vol.32, No.3, pp.178-183.
- [b-EoI] New Zealand Standard: *Evidence of Identity Standard Version 2.0*, 2009.
<<http://www.dia.govt.nz/EOI/pdf/EOIv2.0.pdf>>
- [b-ENISA] ENISA, *Mapping (Interoperable Delivery of European e-government services to public Administrations, Businesses and Citizens) IDABC Authentication Assurance Levels to SAML v2.0*.
- [b-IAF] *Kantara Initiative Identity Assurance Framework v2.0*.
<http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework>
- [b-MOV] Menezes, A., van Oorschot, P. et Vanstone, S. (1997), *Handbook of Applied Cryptography*, pp. 3-4.
<<http://www.cacr.math.uwaterloo.ca/hac/>>
- [b-NeAF] *The National e-Authentication Framework*.
<<http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html>>
- [b-OCDE] OCDE (2007), *Recommandation de l'OCDE sur l'authentification électronique et Orientations pour l'authentification électronique*.
<<http://www.oecd.org/dataoecd/32/45/38921342.pdf>>
- [b-OMB] OMB M-04-04 (2003), *e-Authentication Guidance for Federal Agencies*
<<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>>
- [b-PEA] Industrie Canada (2004), *Principes d'authentification électronique – Cadre canadien*
<http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html>

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication