Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Ligne directrice du gouvernement du Canada (GC) sur l'authentification multifactorielle (AMF) : Recommandations techniques relatives aux authentifiants utilisés pour l'AMF dans le domaine opérationnel du GC

Publié : le 2025-05-23

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

No de catalogue BT48-56/2025F-PDF
ISBN: 978-0-660-76818-2

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Government of Canada (GC) Guideline on Multi-Factor Authentication (MFA): Technical Recommendations for Authenticators to Support MFA Within the GC Enterprise Domain

Ligne directrice du gouvernement du Canada (GC) sur l’authentification multifactorielle (AMF) : Recommandations techniques relatives aux authentifiants utilisés pour l’AMF dans le domaine opérationnel du GC

Sur cette page

Résumé

Les systèmes d'information et les réseaux du gouvernement du Canada (GC) sont des cibles lucratives qui font constamment l'objet d'attaques perpétrées par divers auteurs de cybermenaces. La chef du Centre de la sécurité des télécommunications (CST) a clairement exprimé cette réalité lorsqu'elle a comparu devant le Comité permanent de la sécurité publique et nationale en mars 2018 : « En moyenne, nous bloquons chaque jour plus d'un milliard d'interventions malveillantes visant à compromettre des systèmes gouvernementaux. Un *milliard*. [1] »[traduction]

L'une des techniques les plus couramment utilisées par les auteurs de menaces pour obtenir un accès non autorisé aux systèmes et aux données du GC consiste à compromettre les justificatifs d'identité d'un utilisateur. Les tentatives d'accès non autorisé à des comptes d'utilisateur reposant exclusivement sur l'authentification à un facteur (généralement un identifiant et un mot de passe) rendent les ressources du GC particulièrement vulnérables à la compromission, même lorsque des pratiques appropriées de gestion des justificatifs d'identité sont en place (p. ex., mots de passe robustes et distincts pour chaque compte). En effet, ces justificatifs peuvent toujours être compromis par un certain nombre de moyens comme le piratage psychologique et les maliciels. La mise en œuvre de l'authentification multifactorielle (AMF) est une étape essentielle vers une importante diminution du risque de prise de contrôle des comptes et une amélioration de la posture de sécurité globale du GC. En outre, **tous** les utilisateurs doivent utiliser l'AMF lorsqu'ils accèdent aux ressources du GC pour se conformer à la *Directive sur les services et le numérique* et aux principes de la vérification systématique (zéro confiance).

Le choix d'authentifiants appropriés pour un ministère donné dépend d'une série de facteurs, y compris la capacité de tirer parti des investissements existants, le coût global, l'expérience utilisateur, les

technologies offertes, etc. **En fin de compte, l'objectif est de trouver l'équilibre entre la sécurité, la facilité de gestion, l'interopérabilité, le coût et l'expérience utilisateur afin de déployer des solutions d'AMF appropriées au sein du GC.**

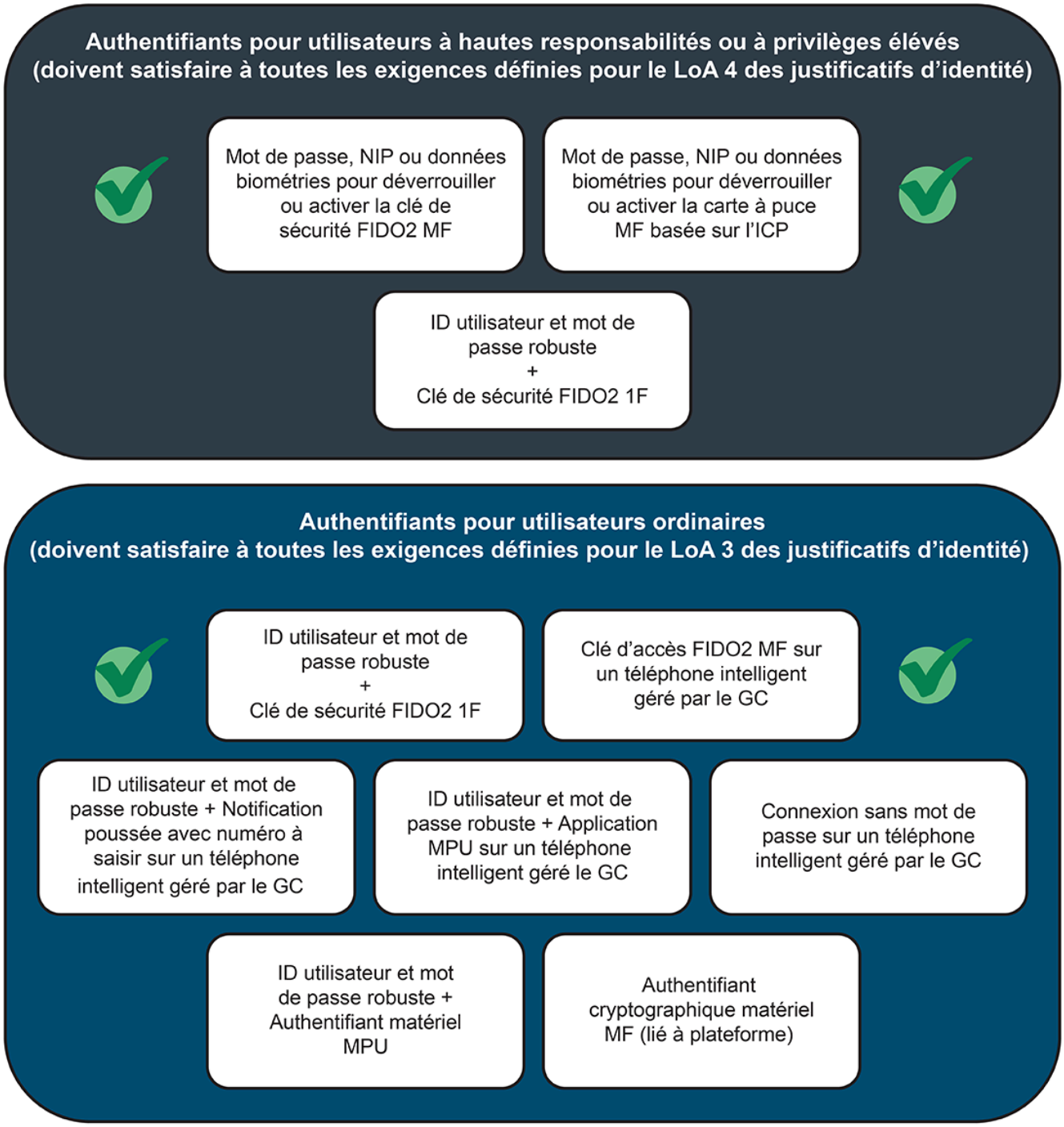
La présente ligne directrice a pour but de définir les exigences techniques associées aux authentifiants et de recommander les authentifiants appropriés à la mise en œuvre de l'AMF dans le domaine opérationnel du GC en tenant compte des considérations relatives à la technologie et à la sécurité. Les exigences techniques sont définies dans les sections 2.2 et 2.3 de la présente ligne directrice et correspondent aux niveaux d'assurance (LoA) des justificatifs indiqués dans la *Norme sur l'assurance de l'identité et des justificatifs*.

La présente ligne directrice recommande que les utilisateurs ordinaires menant des activités opérationnelles au quotidien utilisent des authentifiants qui satisfont à toutes les exigences définies pour le LoA 3 des justificatifs. Il est fortement recommandé d'utiliser des authentifiants qui offrent une résistance à l'hameçonnage (voir la section 2.3.1 pour de plus amples renseignements sur les exigences en matière de résistance à l'hameçonnage). En outre, les utilisateurs à privilèges élevés (administrateurs système, etc.) et les utilisateurs à hautes responsabilités (dirigeant principal des finances, etc.) doivent utiliser des authentifiants qui répondent à toutes les exigences du LoA 4 des justificatifs. Au moins un des authentifiants doit être résistant à l'hameçonnage et indépendant de la plateforme informatique utilisée pour accéder aux ressources du GC.

La figure 1 est un schéma simplifié basé sur la figure 2.2 de la partie principale du présent document qui, de façon générale, définit les authentifiants acceptables et préférés pour les utilisateurs ordinaires ainsi que pour les utilisateurs à hautes responsabilités ou à privilèges élevés.

Comme il s’agit d’une représentation simplifiée, on recommande au lecteur de ne pas l’interpréter hors de son contexte; voir les sections 2.2 et 2.3 pour connaître les exigences et recommandations particulières.

Figure 1 : Vue d’ensemble des authentifiants acceptables et préférés pour deux catégories d’utilisateurs



Les authentifiants marqués d'un ✓ représentent les options préférées pour chaque catégorie d'utilisateurs.

1F = à un facteur
MF = multifactoriel
MPU = mot de passe à usage unique
ICP = infrastructure à clés publiques

▶ Figure 1 - version textuelle

Il convient de noter que la présente ligne directrice porte sur un domaine vaste et complexe, et que tant le contexte des menaces que les technologies et les exigences en matière d'authentification des utilisateurs sont en constante évolution. Les recommandations formulées ci-dessous sont donc susceptibles d'être modifiées au fil du temps. De plus, les mentions de produits ou de fournisseurs ne sont données qu'à titre d'illustration et ne constituent en aucun cas une forme d'approbation officielle par le GC.

En ce qui concerne l'obtention d'authentifiants, les ministères sont censés utiliser des solutions, des actifs et des services de technologie de l'information (TI) pangouvernementaux ou partagés afin d'éviter la redondance, lorsqu'ils sont disponibles et appropriés, comme le précise la section 4.4.2.3 de la *Politique sur les services et le numérique*. À cette fin, les ministères peuvent tirer parti des services d'entreprise qui prennent en charge l'AMF, notamment en utilisant les arrangements en matière d'approvisionnement (AMA) établis par Services partagés Canada (SPC).

1. Introduction

▶ Dans cette section

1.1 Contexte

Les systèmes d'information et les réseaux du gouvernement du Canada (GC) sont des cibles lucratives qui font constamment l'objet d'attaques perpétrées par divers auteurs de cybermenaces. La chef du Centre de la sécurité des télécommunications (CST) a clairement exprimé cette réalité lorsqu'elle a comparu devant le Comité permanent de la sécurité publique

et nationale en mars 2018 : « En moyenne, nous bloquons chaque jour plus d'un milliard d'interventions malveillantes visant à compromettre des systèmes gouvernementaux. Un *milliard*. [2] » [traduction]

L'une des techniques les plus couramment utilisées par les auteurs de menaces pour obtenir un accès non autorisé aux systèmes et aux données du GC consiste à compromettre les justificatifs d'identité d'un utilisateur. Les tentatives d'accès non autorisé à des comptes d'utilisateur reposant exclusivement sur l'authentification à un facteur (A1F) (généralement un identifiant et un mot de passe) rendent les ressources du GC particulièrement vulnérables à la compromission, même lorsque des pratiques appropriées de gestion des justificatifs d'identité sont en place (p. ex., mots de passe robustes et distincts pour chaque compte). En effet, ces justificatifs peuvent toujours être compromis par un certain nombre de moyens comme le piratage psychologique et les maliciels.

La mise en œuvre de l'authentification multifactorielle (AMF) est une étape essentielle vers une importante diminution du risque de prise de contrôle des comptes et une amélioration de la posture de sécurité globale du GC. En outre, l'AMF est un principe fondamental du modèle de sécurité à vérification systématique (zéro confiance), sur lequel le GC s'aligne.

1.2 Objet et portée

Le présent document définit les exigences techniques détaillées associées aux authentifiants et formule des recommandations concernant les authentifiants particuliers qui peuvent être utilisés pour la mise en œuvre de l'AMF dans les domaines opérationnels Non classifié, Protégé A et Protégé B du GC. Bien que certaines des considérations dont il est question dans le présent document s'appliquent également aux entités externes qui accèdent aux services publics du GC, cet aspect n'est pas abordé dans le présent document.

Le présent document est axé sur les considérations relatives à la technologie et à la sécurité, mais il est admis que la détermination des authentifiants les mieux adaptés à un ministère donné (ou à un environnement cible) repose sur de nombreux autres facteurs non technologiques, comme l'expérience utilisateur, le coût, la capacité à tirer parti des investissements existants, etc. Son objectif est de faciliter ce processus en indiquant les authentifiants appropriés que les ministères peuvent choisir pour répondre à leurs besoins particuliers.

Les recommandations formulées dans le présent document se fondent sur des orientations provenant de plusieurs sources, notamment le *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3)* et la version appelée à le remplacer, l'ITSP.30.031 v4 (en cours de rédaction), ainsi que sur les *Digital Identity Guidelines* (version 3) du National Institute of Standards and Technology (NIST), en particulier les publications spéciales (SP pour *Special Publications*) 800-63B et 800-63B-4 (version 4, première version publique) [3]. Certaines des similitudes et des différences entre ces sources sont mises en évidence de manière à améliorer la correspondance entre l'ITSP.30.031 v4 et les lignes directrices du NIST dans le cadre de la collaboration en cours entre le SCT et le Centre canadien pour la cybersécurité (CCC). Lorsque l'ITSP.30.031 v4 sera officiellement publiée, les comparaisons ne seront plus nécessaires, et le présent document pourra être simplifié en conséquence. Les recommandations formulées dans le présent document seront entièrement harmonisées avec l'ITSP.30.031 v4.

Il convient de noter que le présent document porte sur un domaine vaste et complexe, et que tant le contexte des menaces que les technologies et les exigences en matière d'authentification des utilisateurs sont en constante évolution. Il est essentiel de se tenir au courant de ces évolutions et d'adapter les orientations pertinentes en conséquence.

Le présent document n’aborde pas la question de la mise en application des recommandations qu’il contient; on s’attend toutefois à ce que cet objectif soit atteint grâce à une combinaison de politiques, de procédures, de technologies, et de formation et de sensibilisation des utilisateurs.

À noter que le présent document comprend trois annexes. Ces annexes font partie intégrante du document et doivent être lues conjointement avec la partie principale de celui-ci.

Le présent document remplace les *Recommandations pour l’authentification à deux facteurs des utilisateurs dans le domaine opérationnel du gouvernement du Canada.*

Note spéciale sur les authentifiants et les niveaux d’assurance

Il est important de comprendre que le présent document ne traite que des exigences techniques associées aux authentifiants. Il n’aborde pas les questions plus larges associées au processus global d’authentification des utilisateurs. Autrement dit, le niveau d’assurance (LoA) de l’authentifiant (ou de la combinaison d’authentifiants) n’est pas nécessairement le même que celui du processus global d’authentification des utilisateurs, qui pourrait être inférieur, selon les LoA des autres aspects associés à l’authentification (voir l’annexe A pour de plus amples renseignements). Néanmoins, l’adoption d’authentifiants d’AMF appropriés améliorera considérablement la posture de sécurité globale du GC et contribuera à réduire de manière importante la menace de prise de contrôle des comptes d’utilisateurs.

1.3 Public visé

Le présent document est destiné aux praticiens de la sécurité des TI et aux décideurs chargés de déterminer les solutions d'AMF appropriées dans le domaine opérationnel du GC.

1.4 Terminologie

La définition des termes est essentielle à la compréhension du sujet, en particulier quand on sait que les termes clés ne sont pas utilisés de manière uniforme dans les différentes sources (p. ex., le matériel de marketing par rapport aux spécifications techniques correspondantes). Les termes clés utilisés dans le présent document sont définis dans la section 5, l'annexe A (définitions et mises en correspondance des LoA), l'annexe B (termes propres à FIDO Alliance) et l'annexe C (modules de plateforme sécurisée [TPM pour « Trusted Platform Module »]). Les définitions de ces termes clés sont extraites ou dérivées des sources réputées citées en référence, y compris les normes, les spécifications et les orientations pertinentes en matière d'authentification des utilisateurs.

Notez également que les expressions « mot de passe robuste » et « mot de passe robuste et bien géré » utilisées dans le présent document font référence à des pratiques de composition et de gestion des mots de passe qui répondent aux exigences de l'*Orientation sur les mots de passe* du GC.

1.5 Applicabilité

Les recommandations fournies dans le présent document sont destinées aux ministères et organismes du GC dont les systèmes traitent de l'information de niveau Non classifié, Protégé A et Protégé B.

Enfin, les administrateurs généraux sont responsables de « déterminer les exigences en matière de sécurité et de gestion de l'identité pour tous les programmes et services ministériels, en tenant compte des incidences possibles sur les intervenants internes et externes » (voir la section 4.1.4 de la *Politique sur la sécurité du gouvernement*). Le but du présent document est de fournir aux ministères des conseils éclairés afin de les aider à choisir les authentifiants les mieux adaptés à l'AMF en fonction de leurs besoins opérationnels et de leur contexte de menaces particulier. Des exceptions aux recommandations formulées dans le présent document peuvent être accordées sous réserve de l'approbation du Conseil d'examen de l'architecture intégrée du GC (CEAI du GC).

2. Considérations liées aux authentifiants

▶ Dans cette section

Le but de cette section est de définir les concepts et les exigences associés aux authentifiants utilisés pour l'AMF au sein du GC.

2.1 Facteurs d'authentification et types

Comme indiqué dans l'ITSP.30.031 v3 et dans les *Digital Identity Guidelines* du NIST (voir la définition associée dans la NIST SP 800-63-3), un facteur d'authentification est catégorisé comme quelque chose que vous connaissez, quelque chose que vous possédez, ou quelque chose que vous produisez ou qui vous caractérise. Vous trouverez quelques exemples de types d'authentifiants relevant de chaque catégorie dans le tableau 2.1.

Tableau 2.1 : Facteurs d'authentification et exemples

Facteur d’authentification	Exemples de types d’authentifiants
Élément que vous connaissez	• Authentifiants à secret mémorisé (p. ex., un mot de passe [4] associé à un compte d’utilisateur [5])
Élément que vous possédez	• Authentifiants à secret matriciel (p. ex., grille statique ou cartes « bingo ») • Authentifiants hors bande (HB) à un facteur (1F) ou multifactoriels (MF) (p. ex., une notification poussée contenant un numéro à saisir sur un appareil mobile HB comme un téléphone intelligent) • Les authentifiants logiciels ou matériels à mot de passe à usage unique (MPU) 1F ou MF (p. ex., une application MPU sur un dispositif mobile ou un dispositif matériel MPU qui affiche des codes d’authentification à usage unique [6]) • Authentifiants cryptographiques logiciels ou matériels 1F ou MF (p. ex., les authentifiants logiciels ou matériels qui stockent des clés cryptographiques et effectuent des opérations cryptographiques durant le processus d’authentification de l’utilisateur)
Élément que vous produisez ou qui vous caractérise	• Données biométriques associées à une personne qui comprennent à la fois la mesure des caractéristiques physiques (p. ex., empreintes digitales, iris, caractéristiques faciales) et des caractéristiques comportementales (p. ex., cadence de frappe) [7, 8]

Les sections 2.2 et 2.3 ci-dessous fournissent d’autres renseignements concernant les authentifiants et les exigences connexes.

Note spéciale sur la terminologie : authentifiant ou jeton

Avant la publication des *Digital Identity Guidelines* du NIST en 2017, les guides du NIST et du CST sur l'authentification des utilisateurs utilisaient le terme « jeton » (*token*) au lieu d'« authentifiant » (*authenticator*). Les *Digital Identity Guidelines* du NIST ont remplacé le terme par « authentifiant » afin d'éviter toute confusion avec l'utilisation du terme « jeton » dans les technologies et protocoles d'assertion. Le présent document utilise également le terme « authentifiant » plutôt que « jeton », et il est prévu que la prochaine mise à jour du document ITSP.30.031 adopte également cette terminologie.

Note spéciale sur la terminologie : logiciel, matériel et dispositif

Le NIST a ajouté les dispositifs matériels et logiciels à la définition d'un dispositif MPU. Plus précisément, le NIST déclare : « Cette catégorie comprend les dispositifs matériels et les générateurs de MPU logiciels installés sur des dispositifs comme les téléphones cellulaires. » [traduction] Notez que cela s'applique à la fois aux dispositifs MPU 1F et MF. C'est le seul cas où le NIST utilise les termes *matériel* et *logiciel* en parlant d'un « dispositif ». Dans tous les autres cas, le terme « dispositif » désigne uniquement du matériel. Afin d'éviter toute confusion, le présent document utilise le terme « authentifiant » plutôt que « dispositif », que l'authentifiant soit logiciel ou matériel. Notez que, par souci d'uniformité, les extraits des documents du NIST ont été modifiés en fonction de cette terminologie.

2.2 Authentifiants et niveaux d'assurance

L'annexe A donne un aperçu du modèle à quatre niveaux d'assurance (LoA) utilisé par le GC et de la façon dont ces niveaux correspondent à ceux décrits dans les *Digital Identity Guidelines* du NIST. Le lecteur devrait se familiariser avec les concepts décrits dans l'annexe A avant de poursuivre la lecture de la présente section, notamment en ce qui concerne les mises en correspondance entre les niveaux d'assurance des authentifiants (AAL) du NIST et les LoA des justificatifs d'identité du GC. Comme l'indiquent la *Norme sur l'assurance de l'identité et des justificatifs* et l'annexe A, les LoA des justificatifs sont définis comme **le niveau de confiance que la personne a gardé le contrôle des justificatifs qui lui ont été confiés et que ceux-ci n'ont pas été compromis**.

Le tableau 2.2 définit le LoA des justificatifs et l'AAL de chaque type d'authentifiant mentionné dans la NIST SP 800-63B et l'ébauche de l'ITSP.30.031 v4. Bien qu'il existe plusieurs différences entre la NIST SP 800-63B et l'ITSP.30.031 v3, la prochaine mise à jour de l'ITSP.30.031 devrait être étroitement conforme à la NIST SP 800-63B. Les entrées du tableau ci-dessous sont susceptibles d'être modifiées d'ici à la publication officielle de la mise à jour de l'ITSP.30.031 (voir les notes de bas de page et les commentaires associés).

Tableau 2.2 : Authentifiants à chaque AAL/LoA des justificatifs

AAL/LoA les plus élevés possibles	Authentifiants
AAL1/LoA 2 des justificatifs	• Secret mémorisé • Secret matriciel • Authentifiant hors bande à un facteur (HB 1F) • Authentifiant logiciel ou matériel à mot de passe à usage unique à un facteur (MPU 1F) • Authentifiant cryptographique matériel ou logiciel [9] 1F

AAL/LoA les plus élevés possibles	Authentifiants

AAL2/LoA 3 des justificatifs	• Secret mémorisé combiné à un des authentifiants suivants :
	  ◦ Secret matriciel
	  ◦ Authentifiant HB 1F
	  ◦ Authentifiant logiciel ou matériel MPU 1F
	  ◦ Authentifiant cryptographique logiciel1F
	• Authentifiant hors bande multifactoriel (HB MF) [10]
	• Authentifiant cryptographique logiciel MF [11]
	• Authentifiant [12] logiciel ou matériel [13] MF à mot de passe à usage unique (MPU)

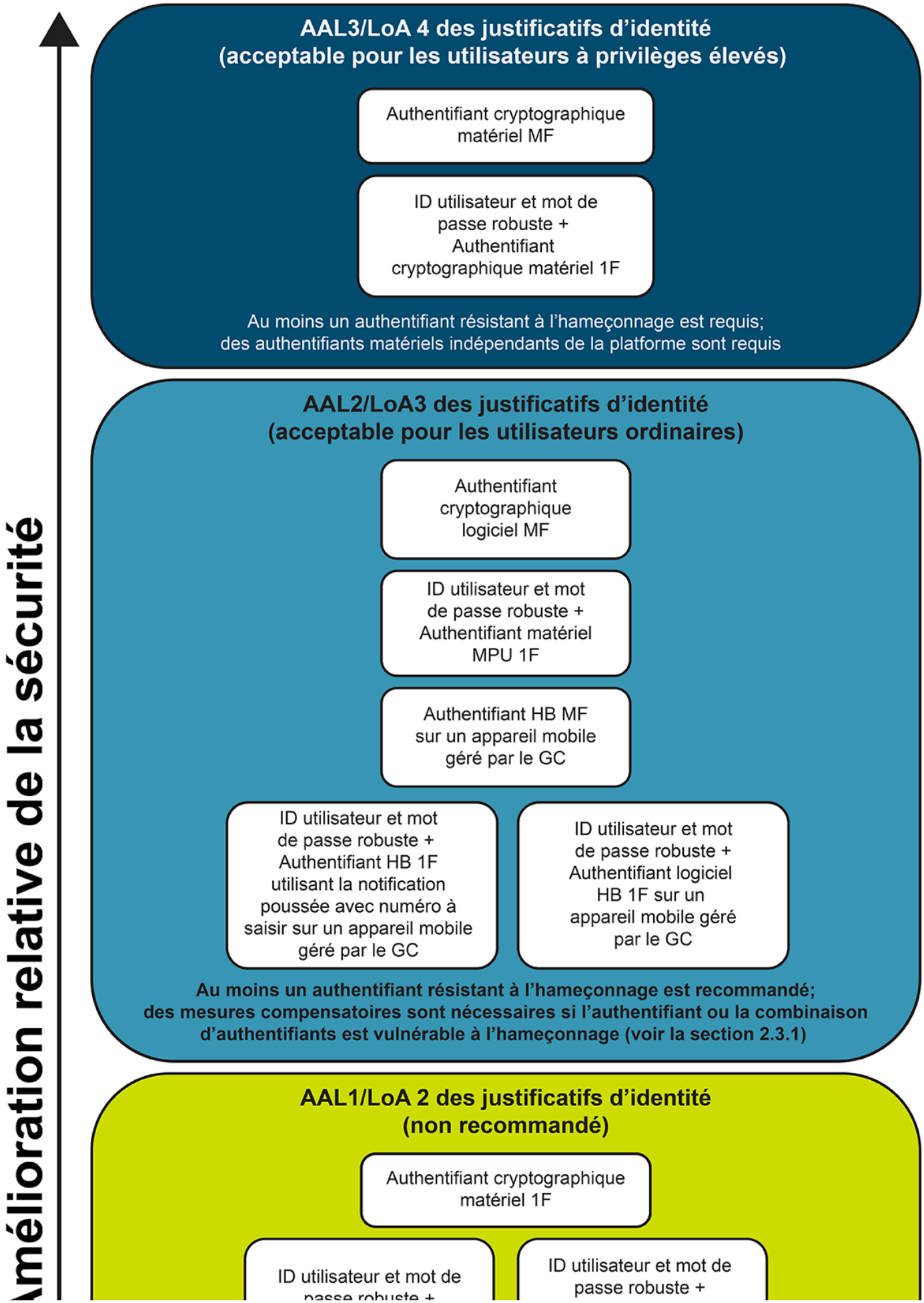
AAL3/LoA 4 des justificatifs	• Authentifiant cryptographique matériel MF • Secret mémorisé combiné à un authentifiant cryptographique matériel 1F [14]

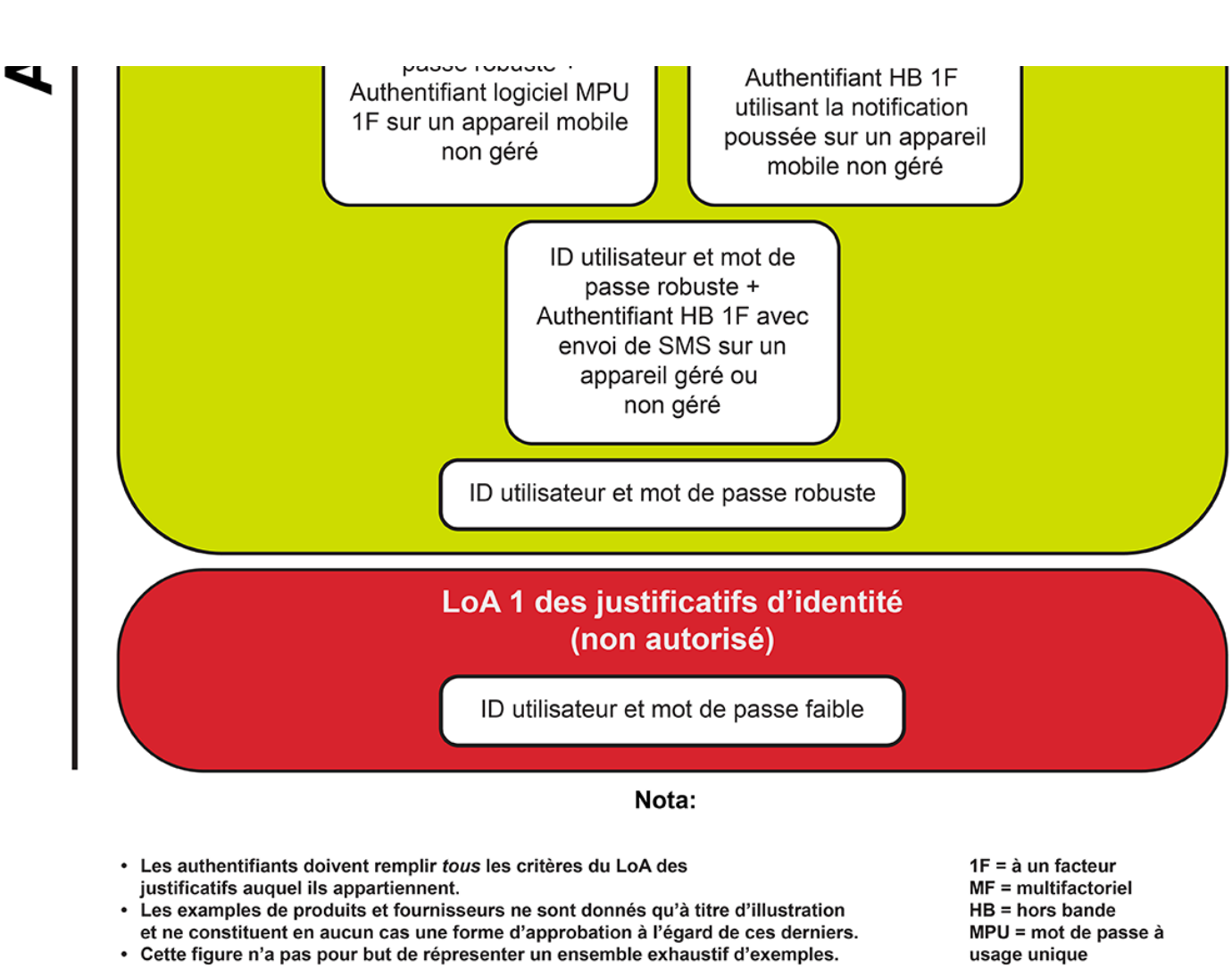
Comme le montrent les entrées du tableau 2.2, l'AMF peut être mise en œuvre au moyen d'un authentifiant MF ou d'une combinaison de deux authentifiants 1F **appropriés**. Il est toutefois important de noter que les authentifiants et les combinaisons d'authentifiants ne sont pas tous équivalents, même s'ils se trouvent au même AAL/LoA des justificatifs d'identité. Autrement dit, certains authentifiants et certaines combinaisons d'authentifiants sont plus robustes que d'autres (du point de vue de la sécurité), même s'ils sont considérés comme étant au même AAL/LoA des justificatifs. Notez également que les authentifiants acceptables utilisés en combinaison ne doivent pas être assujettis au même vecteur d'attaque (méthode de compromission). L'un d'entre eux doit être du type **quelque chose que vous possédez**,qui est protégé contre les reproductions et les duplications. Cela signifie que la quantité de travail nécessaire pour compromettre la combinaison d'authentifiants doit être nettement supérieure à la quantité de travail nécessaire pour compromettre un seul des authentifiants. En outre, tous les dispositifs (plateformes

informatiques, appareils mobiles, authentifiants, etc.) doivent être gérés par le GC (ou en son nom). On s'assure ainsi que les dispositifs utilisés pour accéder aux ressources du GC sont dans l'état requis (l'appareil utilise un logiciel approuvé et à jour, il est doté d'une fonction de détection de logiciels malveillants à jour, rien n'indique qu'il a été compromis, etc.) et qu'ils sont approuvés pour l'utilisation prévue.

La Figure 2.1 présente plusieurs authentifiants et combinaisons d'authentifiants pour chaque AAL/LoA et montre les améliorations relatives en matière de sécurité qu'ils apportent les uns par rapport aux autres à chaque niveau d'assurance. Notez que l'AAL/LoA des justificatifs d'identité associé représente le **niveau le plus élevé possible** qui peut être atteint avec l'authentifiant ou la combinaison d'authentifiants en question et suppose que toutes les exigences applicables à cet AAL/LoA des justificatifs sont satisfaites, comme l'indique la section 3.3. En outre, les comparaisons sont fondées sur les mérites des authentifiants eux-mêmes, indépendamment des autres contrôles de sécurité qui peuvent être mis en œuvre pour leur utilisation. Une justification supplémentaire de leur position relative est fournie dans le tableau 2.3. Veuillez aussi noter qu'il ne s'agit pas d'une série exhaustive d'exemples, mais plutôt d'une représentation des authentifiants susceptibles d'être les plus applicables dans le domaine opérationnel du gouvernement du Canada, en particulier aux AAL2/LoA 3 et AAL3/LoA 4.

Figure 2.1 : Comparaison des authentifiants

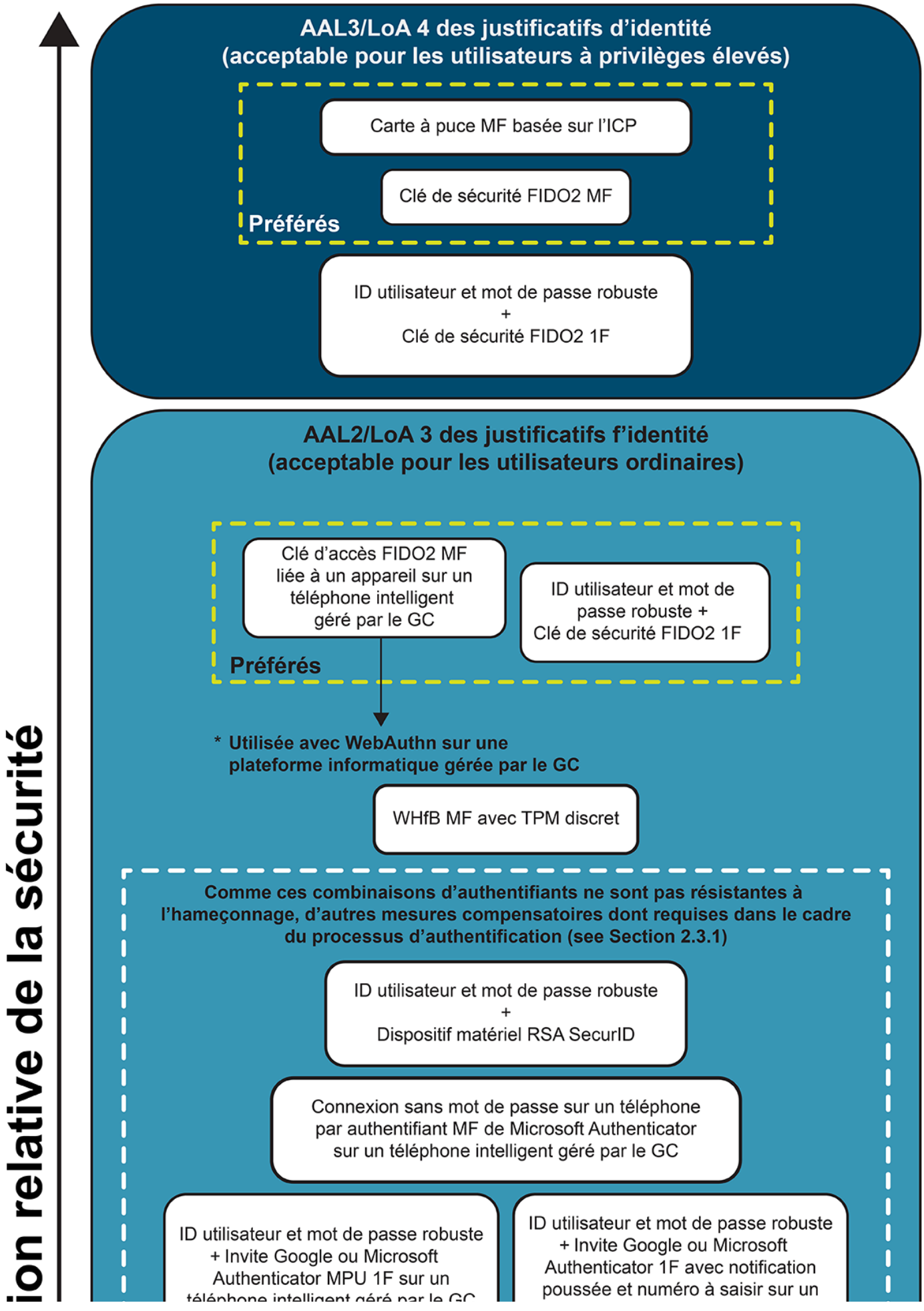

Amélioration relative de la sécurité
AAL3/LoA 4 des justificatifs d'identité
(acceptable pour les utilisateurs à privilèges élevés)
Authentifiant cryptographique matériel MF
ID utilisateur et mot de passe robuste + Authentifiant cryptographique matériel 1F
Au moins un authentifiant résistant à l'hameçonnage est requis;
des authentifiants matériels indépendants de la platforme sont requis
AAL2/LoA3 des justificatifs d'identité
(acceptable pour les utilisateurs ordinaires)
Authentifiant cryptographique logiciel MF
ID utilisateur et mot de passe robuste + Authentifiant matériel MPU 1F
Authentifiant HB MF sur un appareil mobile géré par le GC
ID utilisateur et mot de passe robuste + Authentifiant HB 1F utilisant la notification poussée avec numéro à saisir sur un appareil mobile géré par le GC
ID utilisateur et mot de passe robuste + Authentifiant logiciel HB 1F sur un appareil mobile géré par le GC
Au moins un authentifiant résistant à l'hameçonnage est recommandé;
des mesures compensatoires sont nécessaires si l'authentifiant ou la combinaison d'authentifiants est vulnérable à l'hameçonnage (voir la section 2.3.1)
AAL1/LoA 2 des justificatifs d'identité
(non recommandé)
Authentifiant cryptographique matériel 1F
ID utilisateur et mot de
ID utilisateur et mot de passe robuste +

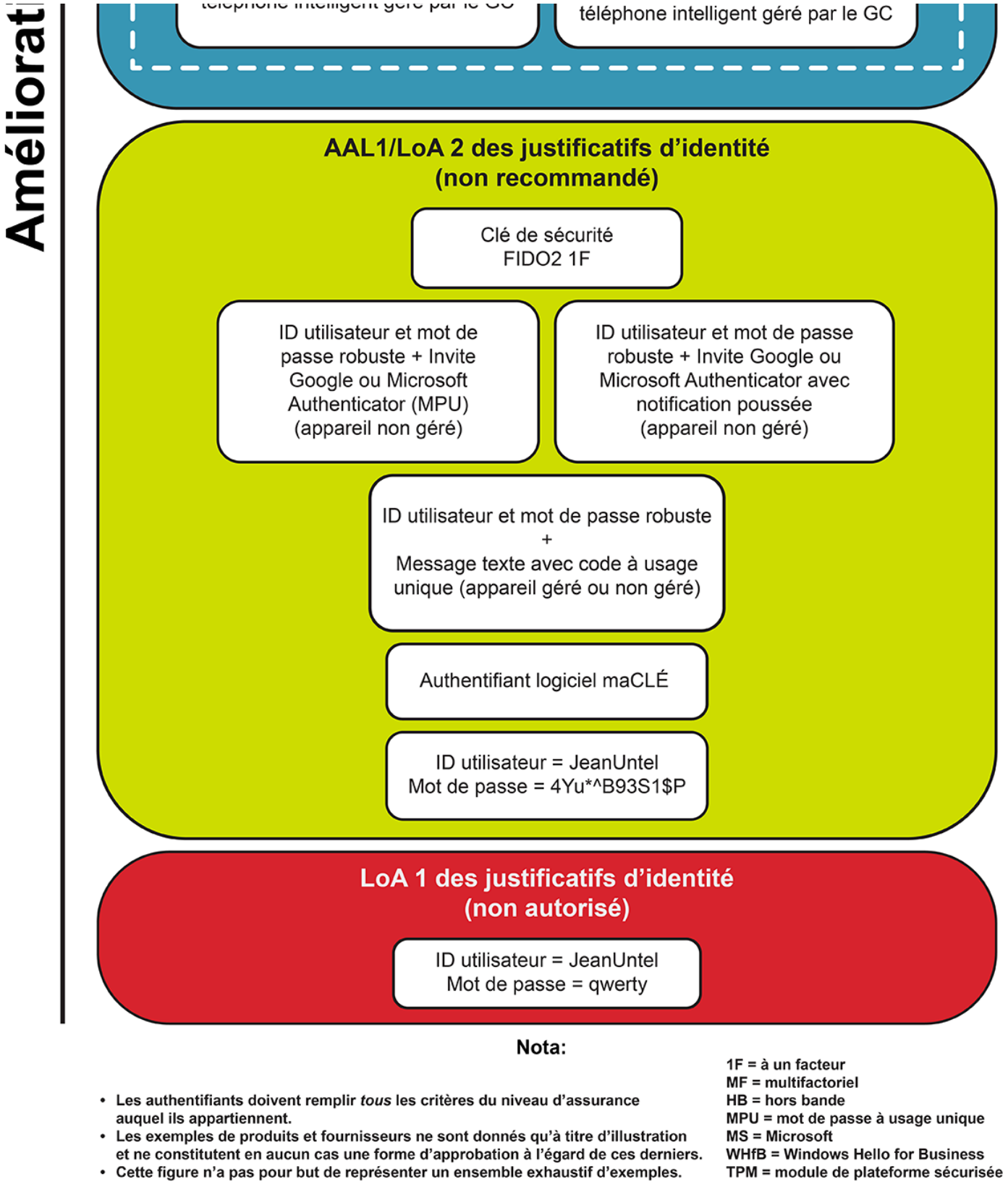


▶ Figure 2.1 - version textuelle

La figure 2.2 développe la figure 2.1 pour illustrer des exemples concrets de différents authentifiants et de différentes combinaisons d'authentifiants. Comme susmentionné, les exemples de produits et fournisseurs ne sont donnés qu'à titre d'illustration et **ne constituent pas une forme d'approbation à l'égard de ces derniers.**

Figure 2.2 : Comparaison d'exemples d'authentifiants


ion relative de la sécurité
AAL3/LoA 4 des justificatifs d'identité
(acceptable pour les utilisateurs à privilèges élevés)
Carte à puce MF basée sur l'ICP
Clé de sécurité FIDO2 MF
Préférés
ID utilisateur et mot de passe robuste
+
Clé de sécurité FIDO2 1F
AAL2/LoA 3 des justificatifs f'identité
(acceptable pour les utilisateurs ordinaires)
Clé d'accès FIDO2 MF
liée à un appareil sur un
téléphone intelligent
géré par le GC
ID utilisateur et mot de
passe robuste +
Clé de sécurité FIDO2 1F
Préférés
* Utilisée avec WebAuthn sur une
plateforme informatique gérée par le GC
WHfB MF avec TPM discret
Comme ces combinaisons d'authentifiants ne sont pas résistantes à
l'hameçonnage, d'autres mesures compensatoires dont requises dans le cadre
du processus d'authentification (see Section 2.3.1)
ID utilisateur et mot de passe robuste
+
Dispositif matériel RSA SecurID
Connexion sans mot de passe sur un téléphone
par authentifiant MF de Microsoft Authenticator
sur un téléphone intelligent géré par le GC
ID utilisateur et mot de passe robuste
+ Invite Google ou Microsoft
Authenticator MPU 1F sur un
ID utilisateur et mot de passe robuste
+ Invite Google ou Microsoft
Authenticator 1F avec notification
poussée et numéro à saisir sur un



▶ Figure 2.2 - version textuelle

Comme l'illustre la figure 2.2, certains authentifiants n'atteignent pas le niveau d'assurance le plus élevé qu'ils pourraient atteindre selon le type duquel ils relèvent (figure 2.1). Le tableau 2.3 justifie la position des

authentifiants et des combinaisons d’authentifiants fournis dans la figure 2.1, ainsi que les exemples fournis dans la figure 2.2.

Veuillez noter que dans le reste de la section 2, l’expression abrégée « AAL/LoA » est utilisée pour désigner « AAL/LoA des justificatifs d’identité ».

Tableau 2.3 : Justification supplémentaire de la position des authentifiants

Authentifiants	Justification supplémentaire de la position dans la figure 2.1	Exemples fournis dans la figure 2.2
Mot de passe faible ou mal géré	Un mot de passe faible ou mal géré est le type d’authentifiant le plus vulnérable, puisqu’il est susceptible de faire l’objet d’un grand nombre d’exploits ou d’attaques et qu’il n’offre qu’un niveau de confiance faible ou nul que l’utilisateur a gardé le contrôle de l’authentifiant et que celui-ci n’a pas été compromis; ce type d’authentifiant faible est au mieux de LoA 1 et ne doit pas être utilisé pour contrôler l’accès aux ressources du GC.	ID utilisateur : JeanUntel Mot de passe : qwerty

Authentifiants	Justification supplémentaire de la position dans la figure 2.1	Exemples fournis dans la figure 2.2
Mot de passe robuste et bien géré	Même si un mot de passe robuste et bien géré offre un certain niveau de confiance que l'utilisateur a gardé le contrôle de l'authentifiant et qu'il est donc considéré de niveau AAL1/LoA 2, il s'agit du plus faible de tous les authentifiants LoA 2. Il est donc positionné à l'extrémité inférieure du LoA 2, puisqu'il est toujours susceptible de faire l'objet de menaces (piratage psychologique, logiciels malveillants, etc.). Compte tenu de l'orientation du GC en matière d'AMF, ce type d'authentifiant ne devrait être utilisé que pour l'AMF, en combinaison avec un autre authentifiant approprié permettant d'atteindre un niveau d'assurance plus élevé (il peut y avoir des exceptions, comme les comptes d'urgence).	ID utilisateur : JeanUntel Mot de passe : 4Yu*^B93S1$P

Authentifiants	Justification supplémentaire de la position dans la figure 2.1	Exemples fournis dans la figure 2.2
Mot de passe robuste combiné à un service de message texte (« SMS ») HB 1F envoyé à un appareil mobile (géré ou non géré)	Même si l'envoi d'un SMS vers un appareil mobile est techniquement une méthode d'authentification HB, il n'est pas considéré de niveau LoA 3 en raison d'un certain nombre de vulnérabilités, comme les faiblesses bien étayées du protocole SS7, et d'autres problèmes comme le détournement du module d'identité de l'abonné (SIM). Il est donc considéré comme à peine meilleur qu'un mot de passe robuste. Notez que l'envoi de SMS n'est pas recommandé comme deuxième facteur, que l'appareil mobile soit ou non géré par le GC.	Un mot de passe robuste combiné à un message texte avec code à usage unique (appareil mobile géré ou non géré)
Mot de passe robuste combiné à une notification poussée HB 1F sur un appareil non géré	Un mot de passe robuste combiné à des notifications poussées sur un appareil mobile non géré est considéré comme AAL1/LoA 2, puisqu'il est impossible de connaître l'état de l'appareil mobile (il peut être compromis). Cependant, il est considéré comme légèrement meilleur qu'un mot de passe robuste combiné à un SMS et est donc positionné un peu plus haut dans le spectre du niveau LoA 2.	Un mot de passe robuste combiné à une invite Google ou Microsoft Authenticator (notification poussée) sur un appareil mobile non géré

Authentifiants	Justification supplémentaire de la position dans la figure 2.1	Exemples fournis dans la figure 2.2
Mot de passe robuste combiné à un authentifiant logiciel (application) MPU 1F sur un appareil non géré	Un mot de passe robuste combiné à une application MPU sur un appareil mobile non géré est considéré de niveau AAL1/LoA 2, puisqu'il est impossible de connaître l'état de l'appareil mobile (il peut être compromis). Cependant, il est considéré comme légèrement meilleur qu'un mot de passe robuste combiné à un SMS et est donc positionné un peu plus haut dans le spectre du LoA 2.	Un mot de passe robuste combiné à une invite Google ou Microsoft Authenticator (MPU) sur un appareil non géré
Authentifiant cryptographique matériel 1F	Un authentifiant cryptographique matériel 1F est considéré comme la meilleure des options AAL1/LoA 2 (même s'il ne s'agit pas d'une méthode d'AMF), puisqu'il est intrinsèquement résistant à l'hameçonnage et aux interceptions (attaque de l'intercepteur) [voir les sections 2.3.1 et 2.3.4]. Il se situe donc à l'extrémité supérieure du spectre AAL1/LoA 2 (en supposant que l'établissement du lien entre l'authentifiant et l'utilisateur est fiable et sûr).	Clé de sécurité FIDO2 1F

Authentifiants	Justification supplémentaire de la position dans la figure 2.1	Exemples fournis dans la figure 2.2
Mot de passe robuste combiné à un authentifiant HB 1F utilisant une notification poussée avec numéro à saisir sur un appareil mobile géré par le GC	Un mot de passe robuste combiné à une notification poussée 1F avec numéro à saisir sur un appareil mobile géré par le GC est considéré de niveau AAL2/LoA 3. Il se situe cependant dans la partie inférieure du spectre LoA 3, puisque cette combinaison d'authentifiants n'est pas intrinsèquement résistante à l'hameçonnage (des mesures compensatoires sont donc nécessaires; voir la section 2.3.1). Même si elle n'est pas représentée dans la Figure 2.1, la notification poussée sans numéro à saisir est considérée comme plus faible que la notification poussée avec numéro à saisir; la notification poussée sans numéro à saisir n'est donc pas recommandée [15]. Cette combinaison d'authentifiants est considérée comme plus ou moins équivalente à un mot de passe robuste combiné à une application MPU sur un appareil mobile géré par le GC (voir l'entrée directement ci-dessous).	Un mot de passe robuste combiné à une invite Microsoft Authenticator (notification poussée avec numéro à saisir) ou Google Authenticator (avec numéro à saisir) sur un appareil mobile géré par le GC (téléphone intelligent)

Authentifiants	Justification supplémentaire de la position dans la figure 2.1	Exemples fournis dans la figure 2.2
Mot de passe robuste combiné à un authentifiant logiciel MPU 1F sur un appareil mobile géré par le GC	Un mot de passe robuste combiné à une application MPU sur un appareil mobile géré par le GC est considéré de niveau AAL2/LoA 3. Il se situe cependant dans la partie inférieure du spectre LoA 3, puisque cette combinaison d'authentifiants n'est pas intrinsèquement résistante à l'hameçonnage (des mesures compensatoires sont donc nécessaires; voir la section 2.3.1). Cette combinaison d'authentifiants est considérée comme plus ou moins équivalente à un mot de passe robuste combiné à une notification poussée avec numéro à saisir sur un appareil mobile géré par le GC (voir l'entrée directement ci-dessus).	Un mot de passe robuste combiné à une invite Microsoft (MPU) ou Google Authenticator sur un appareil mobile géré par le GC (téléphone intelligent)

Authentifiants	Justification supplémentaire de la position dans la figure 2.1	Exemples fournis dans la figure 2.2
Authentifiant HB MF sur un appareil mobile géré par le GC	Un authentifiant HB MF peut atteindre le niveau LoA 3 et est légèrement mieux classé sur le spectre LoA 3 qu'un mot de passe robuste combiné à une notification poussée avec numéro à saisir ou une application MPU, puisqu'il résiste à certaines attaques par piratage psychologique moins sophistiquées. Le canal principal n'est cependant pas protégé contre les interceptions ou l'hameçonnage.	Connexion sans mot de passe par authentifiant MF de Microsoft Authenticator sur un appareil mobile géré par le GC (téléphone intelligent)
Mot de passe robuste combiné à un authentifiant matériel MPU 1F	Un authentifiant matériel MPU 1F combiné à un mot de passe robuste n'est pas résistant à l'hameçonnage, mais il se place plus haut dans le spectre AAL2/LoA 3 que les trois exemples précédents, puisque l'authentifiant matériel MPU n'est pas accessible à distance et qu'il ne peut pas être contourné à distance [16].	Mot de passe robuste combiné à un dispositif matériel MPU RSA SecurID 1F

Authentifiants	Justification supplémentaire de la position dans la figure 2.1	Exemples fournis dans la figure 2.2
Authentifiant cryptographique logiciel MF	Certains authentifiants cryptographiques logiciels MF peuvent atteindre le niveau AAL2/LoA 3, mais pas tous. Pour ce faire, ils doivent remplir toutes les exigences applicables au niveau AAL2/ LoA 3 qui sont décrites dans la section 2.3. Les authentifiants cryptographiques logiciels MF qui ne remplissent pas toutes ces exigences sont considérés de niveau AAL1/LoA 2. L'authentifiant cryptographique logiciel MF maCLÉ n'est qu'un authentifiant AAL1/LoA 2, puisqu'il conserve les clés privées dans un fichier (.epf) plutôt que dans un espace de stockage sécurisé. Il ne remplit donc pas toutes les exigences du niveau AAL2/LoA 3 (voir la section 2.3.2). Le CCC signale également qu'un authentifiant logiciel maCLÉ peut facilement être copié par un auteur de menaces. Une fois qu'il est copié, l'auteur de menaces n'a plus qu'à obtenir le mot de passe ou le NIP utilisé pour déverrouiller l'authentifiant. Cela réduit les propriétés de **quelque chose que vous connaissez** et de **quelque chose que vous possédez** à simplement **quelque chose que vous connaissez**, ce	Deux exemples sont fournis dans la figure 2.2 : • Authentifiant cryptographique logiciel MF maCLÉ légèrement mieux positionné qu'un mot de passe robuste dans le spectre AAL1/LoA 2 • Clé d'accès FIDO2 MF liée à un téléphone intelligent géré par le GC (avec un EEC; voir l'explication dans la cellule précédente à gauche) utilisée conjointement avec WebAuthn sur une plateforme informatique gérée par le GC positionnée à l'extrémité supérieure du spectre AAL2/LoA 3 Même s'il n'est pas illustré dans la figure 2.2, Windows Hello for Business (WHfB) avec TPM microprogramme sur une plateforme informatique gérée par le GC est un exemple d'authentifiant cryptographique logiciel MF qui serait positionné légèrement en dessous de WHfB avec TPM. Cette

Authentifiants	Justification supplémentaire de la position dans la figure 2.1	Exemples fournis dans la figure 2.2
	qui rend l'authentifiant à peine meilleur qu'un mot de passe robuste. Une clé d'accès FIDO2 MF liée à un téléphone intelligent géré par le GC (utilisée conjointement avec WebAuthn sur une plateforme informatique gérée par le GC) se situe à l'extrémité supérieure du spectre AAL2/LoA 3. Elle fait partie des authentifiants préférés, puisqu'elle est résistante à l'hameçonnage et que l'authentifiant lui-même n'est pas lié de manière permanente à la plateforme informatique utilisée pour accéder à la ressource. Veuillez noter que la clé d'accès FIDO2 MF liée à un téléphone intelligent géré par le GC représente deux types d'authentifiants possibles au niveau AAL2/LoA 3, selon que l'authentifiant est pris en charge par un environnement d'exécution de confiance (EEC) ou par un élément sécurisé (ES) intégré. Dans le cas de l'EEC, l'authentifiant est considéré comme un authentifiant cryptographique logiciel MF, et dans le cas de l'ES intégré, comme un authentifiant cryptographique matériel MF (comme indiqué ci-dessous).	situation est similaire à l'utilisation d'un téléphone intelligent géré par le GC pour accéder à une ressource à distance à l'aide d'un authentifiant de plateforme protégé dans un EEC sur le téléphone intelligent en question (en supposant que les plateformes informatiques et les appareils mobiles sont protégés et gérés dans la même mesure).

Authentifiants	Justification supplémentaire de la position dans la figure 2.1	Exemples fournis dans la figure 2.2
	Même si ce dernier est considéré comme plus sûr, les deux sont des choix raisonnables au niveau AAL2/LoA 3.	
Mot de passe robuste combiné à un authentifiant cryptographique matériel 1F	Cette combinaison peut atteindre le niveau AAL3/LoA 4, puisqu'il s'agit d'une solution d'AMF avec au moins un authentifiant résistant à l'hameçonnage et indépendant de la plateforme (en supposant que toutes les autres exigences applicables au niveau AAL3/LoA 4 sont également satisfaites). Le mot de passe doit cependant être envoyé à la partie de confiance (PC) et vérifié par celle-ci, de sorte que cette solution n'est pas préférée au niveau AAL3/LoA 4. Cette combinaison d'authentifiants peut néanmoins constituer une option intéressante au niveau AAL2/LoA 3 et est donc présentée comme l'une des options préférées au AAL2/LoA3 dans la figure 2.2.	Mot de passe robuste combiné à une clé de sécurité FIDO2 1F (apparaît deux fois)

Authentifiants	Justification supplémentaire de la position dans la figure 2.1	Exemples fournis dans la figure 2.2
Authentifiant cryptographique matériel MF	Certains authentifiants cryptographiques matériels MF peuvent atteindre le niveau AAL3/LoA 4, mais pas tous. Pour ce faire, ils doivent remplir toutes les exigences applicables au niveau AAL3/LoA 4 qui sont décrites dans la section 3.3. Même si WHfB avec TPM discret est résistant à l'hameçonnage, il est positionné au niveau supérieur du spectre AAL2/LoA 3 plutôt que AAL3/LoA 4, puisqu'il ne répond pas à l'exigence d'un authentifiant distinct indépendant de la plateforme [17]. Cet aspect le place également légèrement en dessous des autres authentifiants indépendants des plateformes au niveau AAL2/LoA 3. Une clé d'accès FIDO2 MF liée à un téléphone intelligent géré par le GC utilisée conjointement avec WebAuthn sur une plateforme informatique gérée par le GC se situe à l'extrémité supérieure du spectre AAL2/LoA 3. Elle fait partie des authentifiants préférés, puisqu'elle est résistante à l'hameçonnage et que l'authentifiant lui-même n'est pas lié de manière permanente à la plateforme informatique utilisée pour	Quatre exemples sont fournis dans la figure 2.2 : 1. WHfB avec TPM discret (sur une plateforme informatique gérée par le GC) au niveau supérieur du spectre AAL2/LoA 3 2. Clé d'accès FIDO2 MF liée à un téléphone intelligent géré par le GC (avec un ES intégré; voir l'explication dans la cellule précédente à gauche) utilisée conjointement avec WebAuthn sur une plateforme informatique gérée par le GC positionnée légèrement au-dessus de WHfB sur le spectre AAL2/LoA 3 3. Mot de passe, NIP ou données biométriques servant à déverrouiller ou à activer une clé de sécurité FIDO2 MF (utilisée conjointement avec WebAuthn sur une plateforme informatique gérée par le GC) positionné au milieu du spectre AAL3/LoA 4 4. Mot de passe, NIP ou données biométriques servant à déverrouiller

Authentifiants	Justification supplémentaire de la position dans la figure 2.1	Exemples fournis dans la figure 2.2
	accéder à la ressource. Il ne s'agit cependant pas d'un authentifiant AAL3/LoA 4, car un téléphone intelligent n'est pas dédié à la fonction d'authentification comme une clé de sécurité FIDO2 ou une carte à puce basée sur l'infrastructure à clés publiques (ICP). Comme indiqué ci-dessus, il faut aussi un ES intégré au téléphone intelligent pour que cette solution soit considérée comme un authentifiant cryptographique matériel MF. L'utilisation d'un téléphone intelligent équipé d'un EEC est également autorisée au niveau LoA 3, mais cette solution serait considérée comme un authentifiant cryptographique logiciel MF et donc positionnée légèrement plus bas qu'un téléphone intelligent avec un ES intégré. Une clé de sécurité FIDO2 MF est un authentifiant indépendant de la plateforme résistant à l'hameçonnage, ce qui élimine le besoin de transmettre un ID utilisateur et un mot de passe à la PC. Elle se positionne donc plus haut dans le spectre AAL3/LoA 4 qu'un mot de passe robuste combiné avec une clé de sécurité 1F. Une clé de	ou à activer une clé de sécurité FIDO2 MF (utilisée conjointement avec WebAuthn sur une plateforme informatique gérée par le GC) positionné au milieu du spectre AAL3/LoA 4 Même s'il n'est pas illustré dans la Figure 2.2, un téléphone intelligent géré par le GC utilisé pour accéder à une ressource à distance à l'aide d'un authentifiant de plateforme protégé dans un ES intégré sur le téléphone intelligent en question peut être considéré comme équivalent à WHfB avec TPM discret (en supposant que les plateformes informatiques et les appareils mobiles sont protégés et gérés dans la même mesure).

Authentifiants	Justification supplémentaire de la position dans la figure 2.1	Exemples fournis dans la figure 2.2
	sécurité FIDO2 MF est l'un des authentifiants préférés de niveau AAL3/LoA 4, puisqu'elle est à la fois résistante à l'hameçonnage et indépendante de la plateforme et qu'elle ne nécessite pas la transmission d'un mot de passe à la PC. Une carte à puce MF basée sur l'ICP est positionnée au niveau le plus élevé du spectre AAL3/LoA 4, puisqu'il s'agit d'un authentifiant indépendant de la plateforme, résistant à l'hameçonnage et moins sensible à certains vecteurs d'attaque que les autres options AAL3/LoA 4, tout particulièrement si le facteur d'activation ne traverse pas le système d'exploitation, où il pourrait potentiellement être exposé à un auteur de menaces. Une clé de sécurité MF basée sur l'ICP est l'un des authentifiants préférés de niveau AAL3/LoA 4, puisqu'elle est à la fois résistante à l'hameçonnage, indépendante de la plateforme et qu'elle ne nécessite pas la transmission d'un mot de passe à la PC	

Note spéciale sur la vérification centrale ou locale des mots de passe

Comme illustré dans cette section, les secrets mémorisés comme les mots de passe peuvent être combinés avec un autre authentifiant 1F de type quelque chose que vous possédez (p. ex., une notification poussée avec numéro à saisir ou une application MPU) pour obtenir une solution MF et un niveau d'assurance plus élevé. Dans un tel cas, le mot de passe (utilisé comme premier facteur) doit être envoyé à la PC et vérifié par celle-ci (ou en son nom). Il faut donc conserver une représentation du mot de passe (p. ex., hachage salé) de manière centralisée sur un serveur à distance afin que le mot de passe de l'utilisateur puisse être vérifié. D'un autre côté, les authentifiants MF exigent seulement que le mot de passe (ou le NIP) utilisé comme facteur d'activation pour déverrouiller l'authentifiant soit vérifié localement. Comme mentionné dans la section A4 de l'ébauche de la NIST SP 800-63B-4 (version 4, première version publique), la surface d'attaque et les vulnérabilités associées à ces deux scénarios sont différentes à plusieurs égards et doivent être prises en considération lors de la sélection des solutions les plus appropriées. En général, les authentifiants MF doivent être préférés aux combinaisons d'authentifiants qui exigent qu'un mot de passe soit vérifié à distance, dans la mesure du possible.

2.3 Directives de mise en œuvre

La présente section a pour objet de fournir des directives sur la mise en œuvre des authentifiants à chaque niveau AAL/LoA des justificatifs d'identité (« AAL/LoA » dans le reste de la section). Les exigences relatives aux vérificateurs et aux fournisseurs de justificatifs d'identité (FJI) ne sont

pas incluses dans le présent document (ces renseignements se trouvent dans l'ITSP.30.031 v3 et la NIST SP 800-63B). Les définitions des différents termes sont soit copiées, soit dérivées des sources susmentionnées.

2.3.1 Résistance à l'hameçonnage (usurpation d'identité du vérificateur)

Il existe de nombreuses définitions du terme « hameçonnage ». Certaines définitions sont très étroites et se concentrent sur des types d'attaques particuliers, tandis que d'autres sont plus vagues. En général, l'hameçonnage est une tentative par un auteur de menaces de tromper un utilisateur pour qu'il révèle des renseignements sensibles comme des mots de passe ou des numéros de compte bancaire ou pour qu'il fasse quelque chose qu'il ne devrait pas faire, comme cliquer sur un lien malveillant qui télécharge un maliciel sur son dispositif.

Dans le contexte de l'authentification, la résistance à l'hameçonnage se définit comme la capacité du protocole d'authentification de détecter les secrets d'authentification et les résultats valides de l'authentifiant et d'empêcher leur divulgation à une fausse PC, indépendamment du niveau de vigilance de l'utilisateur [18]. Plus particulièrement, les authentifiants résistants à l'hameçonnage offrent une protection robuste contre un type d'attaque d'interception connu sous le nom d'usurpation d'identité du vérificateur. Ce type d'attaque consiste à attirer l'utilisateur vers un faux site Web placé entre l'utilisateur et le vérificateur ou la PC légitime [19]. L'auteur de menaces se fait passer pour le site Web du vérificateur légitime auprès de l'utilisateur, et pour l'utilisateur auprès du vérificateur légitime, afin d'obtenir un accès non autorisé au compte de l'utilisateur ou aux ressources auxquelles l'utilisateur tente d'accéder. La protection contre l'usurpation d'identité du vérificateur est assurée par la liaison du canal ou la liaison du nom du vérificateur.

Veuillez noter que les authentifiants résistants à l'hameçonnage utilisent le chiffrement asymétrique pour résister à l'usurpation d'identité du vérificateur. Les authentifiants qui exigent que l'utilisateur saisisse manuellement les données d'authentification, comme les mots de passe, les authentifiants HB avec saisie de numéro ou les authentifiants MPU, ne résistent pas à l'usurpation d'identité du vérificateur, puisque les données d'authentification ne sont pas liées à la session qui est en cours d'authentification.

Au niveau AAL3/LoA 4, au moins un des authentifiants doit être résistant à l'hameçonnage. Il est également fortement recommandé qu'au moins un des authentifiants AAL2/LoA 3 soit résistant à l'hameçonnage. Cependant, certains authentifiants et certaines combinaisons d'authentifiants autorisés au niveau AAL2/LoA 3 ne sont pas intrinsèquement résistants à l'hameçonnage. Il faut alors mettre en œuvre des mesures de sécurité compensatoires dans le cadre du processus d'authentification afin d'atténuer le risque de réussite des attaques par hameçonnage [20]. Par exemple, s'assurer que l'utilisateur s'authentifie à partir d'un appareil géré par le GC [21], vérifier que l'appareil est configuré correctement et détecter les géolocalisations anormales peut contribuer à compenser l'absence d'authentifiants résistants à l'hameçonnage. De plus, la sensibilisation et la formation des utilisateurs constituent d'importantes mesures d'atténuation qui peuvent contribuer à empêcher l'hameçonnage. Veuillez noter que ces exemples ne constituent pas une liste exhaustive. Comme le contexte des menaces évolue, les mesures de sécurité compensatoires doivent elles aussi évoluer, et les ministères doivent donc procéder à une surveillance continue et aux ajustements nécessaires.

Note spéciale sur l'utilisation de mesures de sécurité compensatoires

Il est important de reconnaître que, pour être efficaces, ces mesures de sécurité supplémentaires doivent être configurées adéquatement. Elles doivent donc être choisies et configurées par des ressources compétentes en matière de sécurité informatique. Les solutions d'authentification fournies par les différents fournisseurs peuvent ne pas prendre en charge les mêmes mesures de sécurité compensatoires ou ne pas les mettre en œuvre au même degré. Au fil du temps, l'introduction de nouvelles options de configuration de la sécurité ou de nouveaux paramètres par défaut peut dégrader ces mesures compensatoires, d'où l'importance de réaliser des évaluations et des essais constants pour garantir leur efficacité continue. La mise en œuvre adéquate de ces mesures peut entraîner des coûts supplémentaires (p. ex., experts-conseils, audits, reprise après une mauvaise configuration, etc.) qui doivent être pris en compte dans le choix de la méthode d'AMF. Pour éviter ces situations, il est fortement recommandé qu'au moins un des authentifiants de AAL2/LoA 3 soit résistant à l'hameçonnage.

Les directives relatives aux authentifiants résistants à l'hameçonnage se résument comme suit :

- AAL1/LoA 2 : aucune précision
- AAL2/LoA 3 : recommandé, sinon des mesures de sécurité supplémentaires doivent être mises en œuvre, comme indiqué ci-dessus
- AAL3/LoA 4 : obligatoire

Autres sources de renseignements sur la résistance à l'hameçonnage [en anglais seulement] :

- Cybersecurity and Infrastructure Security Agency: Implementing Phishing-Resistant MFA

- Office of Management and Budget M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles [22]

2.3.2 Protection des clés cryptographiques

Les authentifiants cryptographiques peuvent utiliser le chiffrement symétrique ou asymétrique et être mis en œuvre de façon logicielle ou matérielle. Dans tous les cas, les clés secrètes (chiffrement symétrique) et les clés privées (chiffrement asymétrique) utilisées durant le processus d'authentification de l'utilisateur doivent être protégées contre toute utilisation, divulgation ou modification non autorisée.

La manière dont les authentifiants cryptographiques protègent les clés cryptographiques dépend de leur type (p. ex., logiciel ou matériel) ainsi que du niveau AAL/LoA où ils sont utilisés. Ces authentifiants peuvent être mis en œuvre de plusieurs façons, notamment au moyen d'un module de plateforme sécurisée (TPM) [23], d'un élément sécurisé (SE) [24] ou d'un environnement d'exécution de confiance (EEC) [25].

L'ITSP.30.031 v3 (voir le tableau 6) et la NIST SP 800-63B (voir les sections 5.1.6.1 à 5.1.9.1) fournissent des conseils sur la protection des clés cryptographiques. Les exigences propres à chaque AAL/LoA incluent ce qui suit :

- AAL1/LoA 2 : Les clés cryptographiques peuvent être conservées sur un disque ou un autre support électronique à condition qu'elles soient robustement protégées contre toute divulgation non autorisée au moyen de contrôles limitant l'accès à la clé aux seuls composants logiciels du dispositif nécessitant l'accès [26].
- AAL2/LoA 3 : Les clés de signature privée appropriées pour TPM, ES ou EEC doivent être générées sur le TPM, l'ES ou l'EEC et ne doivent pas être exportées [27]. Toutes les opérations de chiffrement du processus d'authentification de l'utilisateur doivent être effectuées à l'intérieur

des limites du TPM, de l’ES ou de l’EEC. À ce niveau, il faut également suivre les directives ci-dessous.

    - Les TPM logiciels comme définis par le Trusted Computing Group (voir l’annexe C) ne doivent pas être utilisés et, s’ils sont pris en charge par la plateforme informatique ou l’appareil mobile, ils doivent être désactivés.
    - Les authentifiants cryptographiques logiciels MF qui conservent les clés cryptographiques sur un disque ou un autre support électronique ne sont pas autorisés à partir du niveau AAL2/LoA 3.
    - Il est recommandé que les authentifiants logiciels MPU 1F ou MF utilisés au niveau AAL2/LoA 3 ou supérieur soient exécutés sur un dispositif matériel comme un appareil mobile géré par le GC (téléphone intelligent), physiquement séparé de la plateforme informatique générale.

- AAL3/LoA 4 : Du matériel dédié distinct, comme un TPM discret (voir l’annexe C) ou un ES intégré, est nécessaire. Les clés cryptographiques doivent être générées et conservées de manière sécurisée sur le matériel dédié et ne doivent pas être exportables. Toutes les opérations cryptographiques du processus d’authentification de l’utilisateur doivent être effectuées à l’intérieur des limites du matériel dédié. À ce niveau, il faut également suivre les directives ci-dessous.

    - Des authentifiants matériels indépendants de la plateforme et dédiés à la fonction d’authentification sont nécessaires (p. ex., authentifiant itinérant FIDO2 ou carte à puce basée sur l’ICP) [28]
    - Le facteur d’activation utilisé pour déverrouiller ou activer un authentifiant cryptographique matériel MF, comme une carte à puce basée sur l’ICP, doit être communiqué de manière sécurisée, soit par un chemin de confiance (ne passe pas par le système d’exploitation de la plateforme informatique), soit par la saisie

directe du facteur d’activation sur la carte à puce ou le lecteur de cartes (p. ex., lecteur d’empreintes digitales sur la carte ou le lecteur de cartes).

En outre, pour les authentifiants MF, chaque opération d’authentification nécessite la saisie du facteur d’activation connexe pour déverrouiller ou activer l’authentifiant. La soumission du facteur d’activation doit être une opération distincte du déverrouillage du dispositif hôte (p. ex., plateforme informatique ou téléphone intelligent), même si le facteur d’activation utilisé pour déverrouiller le dispositif hôte peut être utilisé dans l’opération d’authentification [29].

Les exigences de validation des modules cryptographiques sont décrites dans la section 2.3.3 ci-dessous.

2.3.3 Validation des modules cryptographiques

Comme l’indiquent l’ITSP.30.031 v3 et la NIST SP 800-63B, les modules cryptographiques doivent être validés pour répondre aux exigences de la norme FIPS (Federal Information Processing Standard) 140 [30] :

- Les authentifiants cryptographiques utilisés au niveau AAL2/LoA 3 doivent être validés au niveau 1 de la FIPS 140 ou à un niveau supérieur.
- Les authentifiants cryptographiques matériels 1F utilisés conjointement avec un autre authentifiant AAL3/LoA4 doivent être validés au niveau 1 de la FIPS 140 ou à un niveau supérieur dans l’ensemble, avec au minimum une sécurité physique de niveau 3.
- Les authentifiants MF AAL3/LoA 4 doivent être des modules cryptographiques matériels validés au niveau 2 de la FIPS 140 ou à un niveau supérieur, avec au minimum une sécurité physique de niveau 3.

Nota : Il n’y a pas de stipulation au niveau AAL1/LoA 2 pour les authentifiants. Voir la section 4.1.2 de la NIST SP 800-63B pour connaître les exigences relatives aux vérificateurs.

Les authentifiants cryptographiques doivent fonctionner seulement en mode FIPS. Seuls les algorithmes cryptographiques recommandés dans l’ITSP.40.111 doivent être utilisés, et tous les protocoles de sécurité pertinents doivent être configurés comme recommandé dans l’ITSP.40.062.

2.3.4 Résistance à l’interception (attaque de l’intercepteur)

L’interception [31] est une attaque par laquelle l’auteur de menaces s’immisce entre deux parties communicantes afin d’intercepter ou de modifier les données qui circulent entre elles. Dans le contexte de l’authentification, l’auteur de menaces s’immisce entre l’utilisateur et le fournisseur de justificatifs d’identité (FJI) au moment de l’inscription, ou entre l’utilisateur et le vérificateur au moment de la liaison de l’authentifiant [32].

Comme l’indiquent l’ITSP.30.031 v3 et la NIST SP 800-63B, la communication entre l’utilisateur et le vérificateur doit se faire par un canal protégé authentifié (TLS, etc.) pour assurer la confidentialité des données d’authentification et la résistance aux interceptions au niveau AAL1/LoA 2 et aux niveaux supérieurs. Cependant, le niveau de résistance à l’interception peut varier (voir à la description ci-dessous).

Un protocole est considéré comme ayant une faible résistance aux attaques d’interception lorsqu’il dispose d’un mécanisme qui permet à l’utilisateur de savoir s’il interagit avec un vérificateur ou une PC légitime, mais qui fait tout de même courir le risque à l’utilisateur non vigilant de révéler ses données d’authentification à une partie non autorisée, qui les utiliserait ensuite pour usurper l’identité de l’utilisateur auprès du vérificateur ou de la PC légitime. Par exemple, l’envoi d’un mot de passe par TLS authentifié

par un serveur a une faible résistance aux interceptions. Le navigateur Web permet à l'utilisateur de vérifier l'identité du vérificateur ou de la PC, mais si l'utilisateur n'est pas suffisamment vigilant, le mot de passe peut quand même être révélé à une personne non autorisée. Un protocole est dit fortement résistant aux tentatives d'interception s'il ne dépend pas de la vigilance de l'utilisateur pour empêcher la divulgation des données d'authentification à une partie non autorisée qui usurpe l'identité du vérificateur ou de la PC. Un exemple de ce type de protocole est le TLS authentifié par le client, dans lequel le navigateur et le serveur Web s'authentifient mutuellement à l'aide de l'ICP. Les protocoles d'authentification qui peuvent détecter l'usurpation d'identité du vérificateur, comme mentionné dans la section 2.3.1, sont très résistants aux tentatives d'interception.

Conseils particuliers en matière de résistance aux interceptions :

- AAL1/LoA 2 : une faible résistance est requise au minimum
- AAL2/LoA 3 : une faible résistance est requise au minimum; veuillez noter qu'au moins un authentifiant résistant à l'hameçonnage est recommandé, comme indiqué à la section 2.3.1
- AAL3/LoA 4 : une forte résistance est requise et au moins un authentifiant résistant à l'hameçonnage est requis, comme indiqué à la section 2.3.1

2.3.5 Résistance à la réinsertion

On considère qu'un processus d'authentification résiste aux attaques par réinsertion s'il est pratiquement impossible de réussir une authentification en enregistrant puis en réinsérant le message d'une authentification antérieure. Les protocoles qui font appel aux nonces ou aux défis pour prouver la « récence » de la transaction résistent aux attaques par réinsertion. Les authentifiants MPU, les authentifiants cryptographiques et

les secrets matriciels sont des exemples d'authentifiants résistants à la réinsertion. Les secrets mémorisés ne sont pas considérés comme résistants à la réinsertion parce que les données d'authentification (le secret lui-même) sont fournies à chaque authentification [33].

Les conseils relatifs à la résistance à la réinsertion fournis dans l'ITSP.30.031 v3 et la NIST SP 800-63B sont adoptés (à l'exception des conseils modifiés pour le niveau AAL1/LoA 2) comme suit :

- AAL1/LoA 2 : recommandé [34]
- AAL2/LoA 3 : obligatoire
- AAL3/LoA 4 : obligatoire

2.3.6 Intention d'authentification

Les plus récentes directives de la NIST SP 800-63B-4 (deuxième version publique) décrivent l'intention d'authentification comme suit :

> Un processus d'authentification est intentionnel s'il exige du requérant qu'il réponde explicitement à chaque demande d'authentification ou de réauthentification. Le but de l'intention d'authentification est de rendre plus difficile l'utilisation d'authentifiants (p. ex., des authentifiants cryptographiques MF) à l'insu du requérant, par exemple par un maliciel au point terminal. L'authentifiant lui-même **doit** établir l'intention d'authentification, bien que les authentifiants cryptographiques MF **puissent** établir l'intention en réintroduisant le facteur d'activation de l'authentifiant.
>
> L'intention d'authentification **peut** être établie de plusieurs façons. Les processus d'authentification qui requièrent l'intervention du requérant peuvent être utilisés pour prouver l'intention (p. ex., un requérant qui saisit les données produites par un authentifiant MPU). Les authentifiants cryptographiques qui exigent une action de l'utilisateur

pour chaque opération d'authentification ou de réauthentification peuvent également être utilisés pour établir l'intention (p. ex., appuyer sur un bouton ou réinsérer l'authentifiant).

La présentation de caractéristiques biométriques n'établit pas toujours l'intention d'authentification. Par exemple, l'utilisation de la caméra frontale d'un téléphone portable pour capturer des données biométriques faciales ne constitue pas une intention, puisqu'on peut raisonnablement s'attendre à ce que la caméra capture une image du visage lorsque l'appareil est utilisé à d'autres fins que l'authentification. Dans ces scénarios, un mécanisme explicite (p. ex., appuyer sur un bouton logiciel ou physique) **doit** être fourni pour établir l'intention d'authentification.

Les directives du NIST en matière d'intention d'authentification sont adoptées comme suit :

- AAL1/LoA 2 : non obligatoire
- AAL2/LoA 3 : recommandé
- AAL3/LoA 4 : obligatoire

Veuillez noter que si un authentifiant cryptographique matériel 1F est utilisé conjointement avec un mot de passe robuste au niveau AAL3/LoA 4, il faut établir l'intention d'authentification en exigeant une saisie physique de la part de l'utilisateur (p. ex., appuyer sur un bouton) afin que l'authentifiant fonctionne. Le fait d'appuyer sur le bouton pour confirmer la présence physique ne constitue pas un facteur d'authentification supplémentaire.

2.3.7 Considérations propres à FIDO

Un aperçu des spécifications propres à la FIDO Alliance et de la recommandation WebAuthn du W3C, y compris certains détails techniques pertinents pour la présente sous-section, figure à l'annexe B. Le lecteur devrait se familiariser avec la terminologie et les concepts décrits dans l'annexe B avant de poursuivre la lecture de la présente sous-section.

2.3.7.1 Modalité de stockage des justificatifs

Comme indiqué à l'annexe B, les clés privées peuvent être stockées sur l'authentifiant (on parle alors de justificatifs détectables côté client, ou simplement de justificatifs détectables), ou sur le serveur (on parle alors de justificatifs côté serveur) sous forme chiffrée à l'aide d'un puissant algorithme de chiffrement symétrique (la clé symétrique utilisée pour chiffrer les clés privées est générée sur l'authentifiant et n'est jamais exportée). Les compromis entre ces deux modalités de stockage des justificatifs sont examinés à l'annexe B.

Directives concernant les modalités de stockage des justificatifs :

- AAL1/LoA 2 : aucune précision
- AAL2/LoA 3 : justificatifs détectables côté client ou justificatifs côté serveur autorisés [35]
- AAL3/LoA 4 : justificatifs détectables côté client obligatoires; justificatifs côté serveur non autorisés

2.3.7.2 Clés d'accès synchronisées

Comme mentionné à l'annexe B, les justificatifs FIDO peuvent être sauvegardés et copiés (ou synchronisés) sur plusieurs dispositifs. On parle également de justificatifs multidispositifs, mais le terme « clés d'accès synchronisées » semble être le terme plus répandu à l'heure actuelle.

Bien que la mise en œuvre de clés d'accès synchronisées améliore l'expérience de l'utilisateur, la sécurité des clés cryptographiques dépend de leur mise en œuvre par les fournisseurs de services tiers et des méthodes utilisées pour récupérer l'authentifiant. Elle crée également d'autres problèmes, comme l'impossibilité de prendre en charge l'attestation. La prochaine version des normes FIDO2 (en particulier les spécifications WebAuthn Level 3 et Client to Authenticator Protocol [CTAP] 2.2) devrait inclure la prise en charge de l'attestation dans le cadre du processus d'authentification, et pas seulement lors de l'inscription de l'authentifiant, ce qui pourrait conduire à la prise en charge de l'attestation des clés d'accès synchronisées à l'avenir. Le NIST a également publié des directives provisoires sur les « authentifiants synchronisés » (ou clés d'accès synchronisées) en avril 2024, qui ont depuis été incluses dans l'annexe B de la NIST SP 800-63B-4 (deuxième version publique). Sous réserve d'un examen plus approfondi et des conseils du CCC, les clés d'accès synchronisées pourraient être autorisées au niveau AAL2/LoA 3 à l'avenir. Elles ne sont toutefois pas adaptées à des exigences d'assurance plus élevées et ne sont donc pas autorisées au niveau AAL3/LoA 4.

Conseils concernant les clés d'accès synchronisées :

- AAL1/LoA 2 : aucune précision
- AAL2/LoA 3 : non autorisé pour l'instant (mais pourrait changer comme indiqué ci-dessus)
- AAL3/LoA 4 : non autorisé

2.3.7.3 Attestation

Comme indiqué dans la recommandation WebAuthn [en anglais seulement], « l'attestation est employée pour **attester** la **provenance** d'un authentifiant et des données qu'il émet » [traduction]. Les déclarations d'attestation vérifiables sont transmises par l'authentifiant à la PC pendant

l’inscription [36] et permettent de déterminer de manière fiable certaines propriétés de l’authentifiant (p. ex., la marque ou le modèle). Voir le livre blanc sur l’attestation FIDO [en anglais seulement] pour de plus amples renseignements sur l’attestation.

Même si plusieurs types d’attestation sont définis, seules l’attestation de base, l’attestation de l’autorité de certification ou l’attestation d’entreprise doivent être utilisées dans le domaine opérationnel du GC. Les PC doivent préciser (ou exiger) le mode de transmission direct ou d’entreprise (voir la section 5.4.7 de la recommandation WebAuthn).

Notez que l’attestation d’entreprise est un type particulier d’attestation qui est destiné aux déploiements contrôlés au sein d’une entreprise qui souhaite lier les inscriptions à des authentifiants particuliers [37]. L’attestation d’entreprise permet d’identifier de manière unique chaque authentifiant et pourrait devenir le seul type d’attestation autorisé à l’avenir, en particulier au niveau AAL3/LoA 4. Voir l’annexe B pour plus de détails et de références.

Aux niveaux AAL2/LoA 3 et AAL3/LoA 4, l’attestation doit être utilisée pour empêcher l’inscription ou l’utilisation d’authentifiants non approuvés. Les directives concernant les exigences en matière d’attestation sont les suivantes :

- AAL1/LoA 2 : aucune précision (l’attestation n’est pas obligatoire)
- AAL2/LoA 3 : obligatoire
- AAL3/LoA 4 : obligatoire

2.3.8 Résumé des directives de mise en œuvre

Le tableau 2.4 présente un résumé des recommandations formulées dans les sous-sections précédentes. Veuillez noter qu’il s’agit d’un résumé abrégé; la section correspondante doit être consultée pour plus de détails.

Notez également qu’il n’y a aucune précision concernant les authentifiants LoA 1 puisqu’ils ne sont pas autorisés.

Tableau 2.4 : Résumé des directives de mise en œuvre

	AAL1/LoA 2	**AAL2/LoA 3**	**AAL3/LoA 4**
Authentifiants résistants à l’hameçonnage **(voir la section 2.3.1)**	Aucune précision	Recommandé	Obligatoire
Protection des clés cryptographiques **(voir la section 2.3.2)**	Disque ou autre support de stockage électronique autorisé pour les authentifiants cryptographiques logiciels 1F ou MF	TPM, ES ou EEC approprié obligatoire	Matériel dédié obligatoire (p. ex., TPM discret ou ES intégré)
Validation des modules cryptographiques **(voir la section 2.3.3)**	Aucune précision	Niveau global 1	Authentifiant cryptographique matériel MF : niveau global 2 avec sécurité physique de niveau 3 Authentifiant cryptographique matériel 1F : niveau global 1 avec sécurité physique de niveau 3
Résistance à l’interception **(voir la section 2.3.4)**	Obligatoire	Obligatoire	Obligatoire

	AAL1/LoA 2	AAL2/LoA 3	AAL3/LoA 4
Résistance à la réinsertion **(voir la section 2.3.5)**	Recommandé	Obligatoire	Obligatoire
Intention d'authentification (voir la section 2.3.6)	Non obligatoire	Recommandé	Obligatoire
Modalité de stockage des justificatifs **(voir la section 2.3.7.1)**	Aucune précision	Justificatifs détectables côté client ou justificatifs côté serveur autorisés	Justificatifs détectables côté client obligatoires (clés d'accès liées à un appareil seulement)
Clés d'accès synchronisées **(voir la section 2.3.7.2)**	Aucune précision	Non autorisé à l'heure actuelle (pourrait changer)	Non autorisé (clés d'accès liées à un appareil seulement)
Attestation **(voir la section 2.3.7.3)**	Aucune précision	Obligatoire	Obligatoire

2.4 Autres considérations

Le but de cette section est d'exposer les considérations techniques supplémentaires qui doivent être prises en compte dans le cadre d'une solution d'authentification complète, en plus des aspects techniques associés aux authentifiants dans la section 2.3. Il ne s'agit pas d'une liste

exhaustive, et les sujets ne sont pas traités en profondeur. D'autres points devront être pris en considération dans le cadre des initiatives d'AMF du GC.

2.4.1 Liaison des authentifiants

Il est essentiel de lier les authentifiants à une identité particulière pour garantir que le bon utilisateur accède aux bonnes ressources (p. ex., comptes, applications, services et information). La liaison d'un utilisateur à un ou à plusieurs authentifiants se fait au cours de la procédure d'inscription de l'utilisateur, mais on peut aussi le faire ultérieurement en utilisant les authentifiants déjà émis pour lier de nouveaux authentifiants.

La section 6.1 de la NIST SP 800-63B contient des directives relatives à la liaison des authentifiants. La section 6.1.2.1 de la NIST SP 800-63B traite de l'utilisation d'authentifiants à un niveau d'assurance donné pour lier d'autres authentifiants à un LoA identique ou inférieur. La section 6.1.2.2 de la NIST SP 800-63B traite de la possibilité d'utiliser un authentifiant 1F pour ajouter un autre type d'authentifiant 2F, ce qui peut faire passer le niveau d'assurance de AAL1/LoA 2 à AAL2/LoA 3 (selon les authentifiants). Par exemple, un utilisateur peut s'authentifier auprès d'un service Web à l'aide d'un ID utilisateur et d'un mot de passe préalablement enregistrés, puis inscrire un authentifiant de type **quelque chose que vous possédez** (p. ex., un authentifiant FIDO) qui sera désormais utilisé comme deuxième facteur [38].

L'utilisation d'un ID utilisateur et d'un mot de passe existants pour lier un authentifiant 2F supplémentaire ne garantit pas que le compte de l'utilisateur n'a pas déjà été compromis. L'utilisateur qui tente d'inscrire un authentifiant supplémentaire peut très bien être un imposteur. Bien que le NIST recommande qu'une notification de l'événement soit envoyée à l'utilisateur par une méthode HB (p. ex., compte de courrier électronique

inscrit), cette mesure ne suffit pas nécessairement à détecter la compromission d'un compte. Il faut donc prendre des mesures supplémentaires pour s'assurer que l'utilisateur est bien celui qu'il prétend être. Cela est possible si le deuxième facteur est déjà lié à l'utilisateur (p. ex., un téléphone intelligent géré par le GC et remis à l'utilisateur doit être utilisé comme deuxième facteur). Si le deuxième authentifiant n'a pas été préalablement lié à l'utilisateur, d'autres méthodes doivent être employées. Par exemple, il est possible d'utiliser la vérification d'un code d'accès unique envoyé ou fourni au **bon** utilisateur par un moyen fiable HB pour augmenter le niveau de confiance selon lequel l'utilisateur qui réalise l'inscription est bien celui qu'il prétend être. Le mécanisme HB doit être limité dans le temps (p. ex., expiration dans les 10 jours ouvrables).

2.4.2 Récupération des authentifiants

Des mécanismes appropriés de récupération des authentifiants doivent être mis en place pour rétablir l'accès de l'utilisateur en cas de perte, de vol ou de détérioration d'un authentifiant existant. Les méthodes de récupération varient en fonction du type d'authentifiant, mais dans tous les cas, elles doivent être au moins aussi robustes et sûres que la ou les méthodes utilisées pour établir la liaison d'origine avec l'authentifiant. La section 6.1.2.3 de la NIST SP 800-63B fournit des directives supplémentaires concernant la récupération des authentifiants. Les utilisateurs doivent également être informés de leurs responsabilités, notamment en ce qui concerne le signalement immédiat des authentifiants perdus ou volés (voir la section 6.2 de la NIST SP 800-63B pour de plus amples renseignements).

Veuillez noter que d'autres considérations relatives à la gestion du cycle de vie des authentifiants doivent également être prises en compte, notamment le renouvellement (section 6.1.4 de la NIST SP 800-63B), la suspension (section 6.2 de la NIST SP 800-63B), l'expiration (section 6.3 de la NIST SP 800-63B) et la révocation (section 6.4 de la NIST SP 800-63B).

2.4.3 Réauthentification

La réauthentification sert à déterminer si l'utilisateur précédemment authentifié est toujours présent dans une session donnée, soit parce qu'il est inactif, soit après un certain laps de temps. Les lignes directrices des *Digital Identity Guidelines* du NIST (voir les sections 4.1.3, 4.2.3, 4.3.3 et 7.2 de la NIST SP 800-63B) décrivent les exigences en matière de réauthentification à chaque AAL. Ces exigences sont adoptées avec les précisions supplémentaires suivantes [39] :

- AAL1/LoA 2 : La réauthentification est requise au moins tous les 30 jours, que l'utilisateur soit actif ou non; les PC sont libres de déterminer leurs propres exigences en matière de délai d'inactivité, s'il y a lieu.
- AAL2/LoA 3 : La réauthentification est requise au moins toutes les 12 heures, que l'utilisateur soit actif ou non; la réauthentification est également requise après 30 minutes d'inactivité de l'utilisateur (bien que l'utilisateur puisse être invité à confirmer qu'il est toujours présent avant que le délai d'inactivité ne soit écoulé [40]); la réauthentification d'une session qui n'a pas encore atteint sa limite de temporisation peut se faire au moyen d'un secret mémorisé ou de données biométriques conjointement avec le secret de session encore valide.
- AAL3/LoA 4 : La réauthentification est requise au moins toutes les 12 heures, que l'utilisateur soit actif ou non; la réauthentification est également requise après 15 minutes d'inactivité (bien que l'utilisateur puisse être invité à confirmer qu'il est toujours présent avant que le délai d'inactivité ne soit écoulé [41]); la réauthentification nécessite une AMF.

Si l'utilisateur ne se réauthentifie pas avec succès dans la minute qui suit la demande de réauthentification, la session est interrompue. Si la réauthentification est réussie, les limites de temporisation de la session et le délai d'inactivité de l'utilisateur sont réinitialisés.

Le NIST souligne (voir la NIST SP 800:63 Digital Identity Guidelines – Frequently Asked Questions) qu'il y a d'autres moyens de s'assurer que le dispositif n'est pas utilisé par une partie non autorisée, comme le verrouillage au niveau du système d'exploitation et l'authentification locale obligatoire pour que l'utilisateur puisse déverrouiller l'appareil. Il n'est pas toujours possible pour une PC de connaître l'état du dispositif de l'utilisateur et, dans ce cas, les limites de temporisation constituent une mesure de contrôle raisonnable. Si la PC sait que l'utilisateur utilise un système géré qui exige le verrouillage de l'écran selon les stratégies programmées, elle peut être en mesure d'assouplir les limites de temporisation du système en question. Une PC pourrait aussi gérer la plupart des interactions de l'utilisateur à un certain AAL et passer à un AAL supérieur pour les opérations de nature délicate. Dans un tel cas, la session à privilèges limités pourrait durer beaucoup plus longtemps que celle à privilèges plus élevés. L'adoption de mesures compensatoires comme celles-ci fait partie du processus d'évaluation des risques.

[Nota : Si la section 7.2.1 de la NIST SP 800-63B traite de l'exigence pour une PC de transmettre l'âge maximal d'authentification à un fournisseur d'identité ou de justificatifs (FID/FJI) dans un scénario fédéré, elle n'aborde pas la possibilité de forcer la réauthentification, qui est prise en charge par les protocoles de fédération SAML et OpenID Connect. Les PC peuvent utiliser ces derniers pour forcer la réauthentification quel que soit l'état de la session authentifiée entre l'utilisateur et le FID. Heureusement, l'ébauche de la version 4 des *Digital Identity Guidelines* du NIST a ajouté la notion d'authentification forcée à la section 5.6 de la SP-800-63C-4.]

2.4.4 Authentification renforcée

L'authentification renforcée, qu'il ne faut pas confondre avec la réauthentification décrite dans la sous-section précédente, est utilisée lorsqu'il est nécessaire d'élever le LoA d'une session donnée (p. ex., l'utilisateur est authentifié au LoA 2 et demande l'accès à une ressource qui nécessite une authentification LoA 3). Les PC doivent être en mesure d'inviter l'utilisateur à s'authentifier au LoA supérieur (ou de le rediriger vers un FID dans un environnement fédéré) afin de renforcer l'authentification en cas de besoin.

2.4.5 Authentification centralisée

Comme indiqué dans le document *Considérations et stratégie d'authentification multifactorielle des services organisationnels de TI du GC*, une solution organisationnelle centralisée d'authentification, qui peut prendre en charge plusieurs méthodes d'AMF fondées sur des normes ouvertes et acceptées par l'industrie, est un élément essentiel de la stratégie globale de gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) du GC. L'authentification doit être centralisée dans toute la mesure du possible pour alléger le fardeau de la prise en charge de plusieurs mécanismes d'authentification des applications et des services individuels, prendre en charge l'identification unique et permettre la constitution d'une fédération. L'authentification centralisée facilite également le contrôle d'accès continu en fonction du risque, comme nous le verrons dans la sous-section suivante.

2.4.6 Contrôle d'accès en fonction du risque

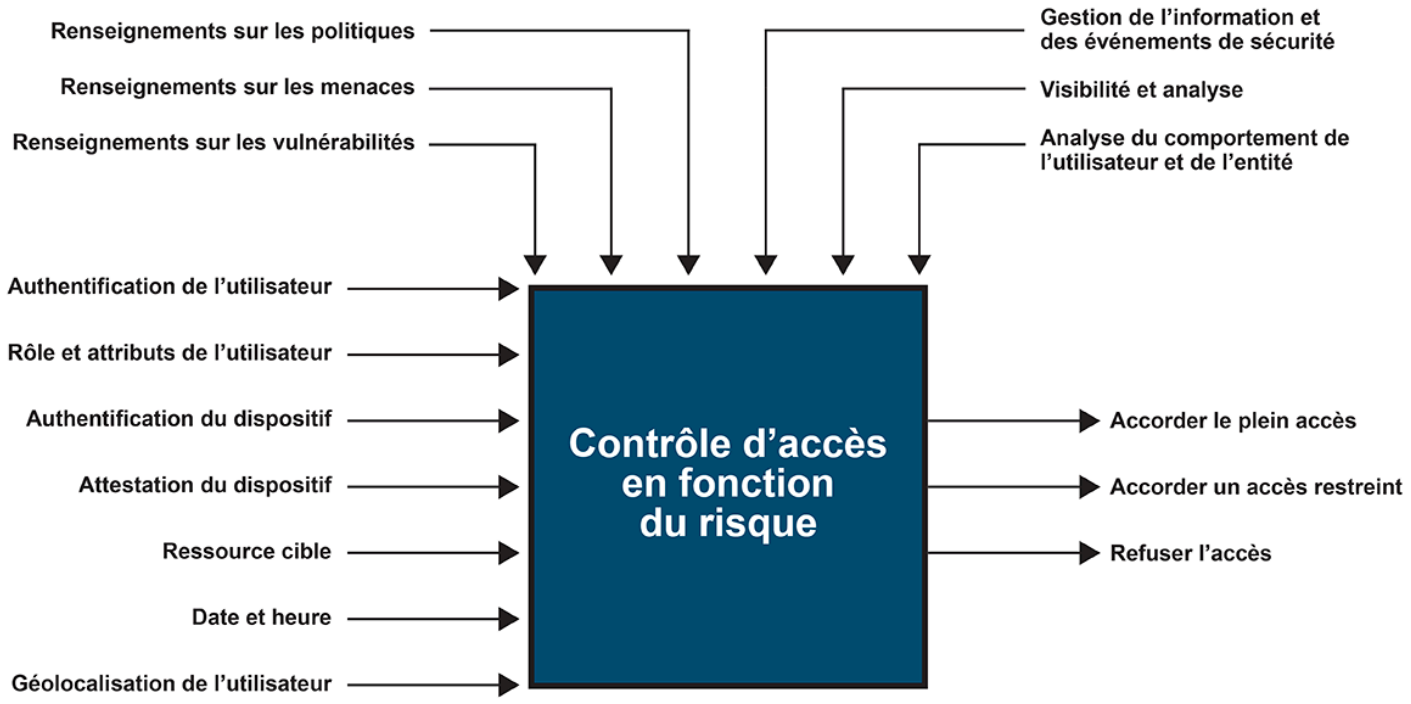
Le contrôle d'accès en fonction du risque (ou simplement le contrôle d'accès adaptatif) est un modèle de contrôle d'accès dynamique qui utilise de multiples indicateurs de sécurité pour éclairer la prise de décisions

entourant le contrôle d’accès, comme la force de la méthode d’authentification de l’utilisateur, le niveau d’assurance de la session établie entre le système et l’utilisateur, la géolocalisation de l’utilisateur et d’autres considérations [42].

Même s’il ne s’agit pas d’une représentation exhaustive, la Figure 2.3 aide à comprendre le concept d’un modèle de contrôle d’accès en fonction du risque. Comme l’illustre le schéma, l’authentification de l’utilisateur n’est que l’une des nombreuses considérations qui motivent les décisions en matière de contrôle d’accès. Par exemple, l’attestation du dispositif est un complément important de l’authentification de l’utilisateur, puisqu’il s’agit d’une façon fiable et sûre de vérifier l’identité et l’état du dispositif utilisé pour accéder aux ressources du GC.

Les décisions en matière de contrôle d’accès doivent être dynamiques et s’adapter aux changements de politique et à l’évaluation des menaces et des risques en temps réel, comme l’illustrent les données d’entrée politiques et télémétriques dans la Figure 2.3. Ce modèle constitue le fondement même d’un contrôle d’accès continu en fonction du risque en application des principes de la vérification systématique [43]. Il permet également de mettre en place des mesures compensatoires de manière à compenser les faiblesses dans un domaine par d’autres domaines et d’éclairer le processus global de prise de décisions en matière de contrôle d’accès.

Figure 2.3 : Modèle conceptuel du contrôle d’accès en fonction du risque



▶ Figure 2.3 - version textuelle

2.4.7 Utilisation de la biométrie

Comme indiqué dans les *Digital Identity Guidelines* du NIST (voir la section 5.2.3 de la NIST SP 800-63B), « la biométrie DOIT être utilisée seulement dans le cadre d'une authentification multifactorielle avec un authentifiant physique (**quelque chose que vous possédez**). » [traduction] Par conséquent, la biométrie ne peut être utilisée comme second facteur qu'en combinaison avec quelque chose que l'utilisateur possède, comme un authentifiant cryptographique matériel MF doté d'un capteur intégré (p. ex., un lecteur d'empreintes digitales). Lorsque la biométrie est utilisée comme second facteur, certaines exigences s'appliquent concernant le taux de fausses correspondances et les technologies de détection des attaques de présentation (p. ex., détection du caractère vivant).

Il faut aussi noter que certaines technologies biométriques sont conçues dans un souci de commodité pour l'utilisateur plutôt que de sécurité et, par conséquent, peuvent ne pas convenir au niveau d'assurance requis. Il faut donc être prudent lors de l'utilisation de la biométrie comme facteur d'authentification. Voir la section 5.2.3 de la NIST SP 800-63B pour de plus amples renseignements.

2.4.8 Prenez vos authentifiants personnels (PAP)

Comme indiqué précédemment dans la section 2.2, tous les dispositifs utilisés pour accéder aux ressources internes du GC doivent être gérés par le GC. Cela inclut les appareils mobiles comme les téléphones intelligents. Il est cependant admis que certains ministères n'ont pas d'autre choix que de mettre en œuvre l'AMF sur des appareils personnels, en particulier pour les entrepreneurs. Bien que l'AMF ajoute une mesure de sécurité supplémentaire par rapport à une solution 1F basée seulement sur un ID utilisateur et un mot de passe, un appareil mobile non géré par le GC est plus susceptible d'être compromis qu'un appareil géré par le GC. Toutefois, la gestion des appareils mobiles, la gestion unifiée des points terminaux (UEM) ou la gestion des applications mobiles pourraient potentiellement être utilisées pour gérer les données et les applications ministérielles sur les appareils mobiles personnels, ce qui réduirait considérablement le risque par rapport aux appareils non gérés. Utilisé conjointement avec une plateforme informatique gérée par le GC, ce système pourrait éventuellement faire passer le niveau d'assurance de LoA 2 à LoA 3, pourvu que les mesures de sécurité et les pratiques exemplaires appropriées soient en place (p. ex., la séparation entre l'espace de travail et l'espace personnel est maintenue en permanence, les dispositifs débridés et compromis sont détectés, etc.). Voir *Sécurité des appareils des utilisateurs finaux pour les modèles de déploiement Prenez vos appareils personnels (PAP) – ITSM.70.003* pour de plus amples renseignements.

Dans tous les cas, il est préférable d'utiliser les méthodes d'authentification les plus robustes possibles. Par exemple, l'utilisation de messages texte (SMS) est fortement déconseillée. Il vaut mieux utiliser des mécanismes plus sécuritaires comme la notification poussée avec saisie de numéro ou une application MPU. L'utilisation d'authentifiants résistants à l'hameçonnage, comme les clés d'accès FIDO2 liées à un appareil et conservées sur l'appareil mobile de l'utilisateur ou une clé de sécurité FIDO2 appartenant à l'utilisateur (l'une ou l'autre pouvant être utilisée pour s'authentifier avec WebAuthn sur une plateforme informatique gérée par le GC), peut également être une option. Si cette méthode est adoptée, il faut aussi utiliser l'attestation pour vérifier que l'authentifiant répond aux exigences minimales à remplir pour accéder à la ressource cible. Il convient également de noter que l'utilisation d'un dispositif personnel en tant qu'authentifiant ne doit pas créer involontairement la possibilité d'accéder aux ressources internes du GC à l'aide de ce dispositif. Plus particulièrement, les authentifiants « Prenez vos authentifiants personnels » (PAP) devraient être utilisés en combinaison avec une plateforme informatique gérée par le GC.

Les cas d'utilisation et la nécessité d'avoir des mesures d'atténuation des risques supplémentaires devraient être pris en compte avant l'adoption d'une méthode PAP. Les considérations relatives à la protection de la vie privée doivent également être évaluées.

3. Résumé et recommandations

Le présent document fournit des conseils techniques détaillés concernant les authentifiants et recommande les authentifiants appropriés à la mise en œuvre de solutions d'AMF dans le domaine opérationnel du GC :

- Pour les utilisateurs ordinaires menant des activités opérationnelles quotidiennes, le ou les authentifiants doivent satisfaire à toutes les exigences définies pour le AAL2/LoA 3. Même si certains des authentifiants acceptables au niveau AAL2/LoA 3 ne sont pas résistants à l'hameçonnage, il est fortement recommandé qu'au moins un des authentifiants le soit. Si l'authentifiant (ou la combinaison d'authentifiants) n'offre pas de résistance à l'hameçonnage, des mesures compensatoires, comme indiqué dans la section 2.3.1, doivent être mises en œuvre pour atténuer le risque que les justificatifs d'identité de l'utilisateur soient compromis par des tentatives d'hameçonnage. Il est également recommandé qu'un des authentifiants soit physiquement séparé de la plateforme informatique ou du dispositif utilisé pour accéder à la ressource cible. Dans tous les cas, les plateformes informatiques, les appareils mobiles et les authentifiants doivent être gérés par le GC (ou en son nom). Les authentifiants préférés sont :
    - les clés d'accès FIDO2 MF résistantes à l'hameçonnage liées à un appareil [44] sur un téléphone intelligent géré par le GC (utilisé pour s'authentifier auprès d'une PC à distance par l'entremise de WebAuthn sur une plateforme informatique distincte);
      ou
    - un mot de passe robuste et bien géré [45] (fourni à la PC) combiné à une clé de sécurité FIDO2 1F résistante à l'hameçonnage et dotée d'un bouton-poussoir permettant de vérifier la présence physique (utilisé pour s'authentifier auprès de la PC par l'entremise de WebAuthn sur une plateforme informatique distincte).

  D'autres authentifiants acceptables peuvent être utilisés pour l'AMF des utilisateurs ordinaires :

    - Windows Hello for Business avec un TPM (déverrouillé par l'utilisateur avec un facteur d'activation comme un NIP ou des données biométriques).
    - Un mot de passe robuste et bien géré, combiné à un authentifiant matériel MPU 1F (p. ex., dispositif matériel RSA SecurID) avec des mesures de sécurité supplémentaires mises en œuvre dans le cadre du processus d'authentification pour compenser l'absence d'authentifiants résistants à l'hameçonnage.
    - Un authentifiant HB MF sans mot de passe (p. ex., l'application MS Authenticator utilisant la méthode d'authentification par connexion téléphonique) avec des mesures de sécurité supplémentaires mises en œuvre dans le cadre du processus d'authentification afin de compenser l'absence d'authentifiants résistants à l'hameçonnage.
    - Un mot de passe robuste et bien géré, combiné à une application MPU (p. ex., Google Authenticator ou MS Authenticator utilisant la méthode d'authentification MPU) avec des mesures de sécurité supplémentaires mises en œuvre dans le cadre du processus d'authentification afin de compenser l'absence d'authentifiants résistants à l'hameçonnage.
    - Un mot de passe robuste et bien géré, combiné à une notification poussée avec numéro à saisir (p. ex., invite Google ou MS Authenticator avec la méthode d'authentification par notification poussée) avec des mesures de sécurité supplémentaires mises en œuvre dans le cadre du processus d'authentification afin de compenser l'absence d'authentifiants résistants à l'hameçonnage.
- Les utilisateurs à privilèges élevés (administrateurs système, etc.) et les utilisateurs à hautes responsabilités (dirigeant principal des finances, etc.) doivent utiliser des authentifiants qui satisfont à toutes les exigences du niveau AAL3/LoA 4 des justificatifs d'identité. Il faut

utiliser au moins un authentifiant résistant à l'hameçonnage et un authentifiant qui est indépendant physiquement de la plateforme informatique ou du dispositif utilisé pour accéder aux ressources cibles. Dans tous les cas, les plateformes informatiques, les appareils mobiles et les authentifiants doivent être gérés par le GC (ou en son nom). Les authentifiants préférés sont :

- une carte à puce MF basée sur l'ICP résistante à l'hameçonnage; ou
- une clé de sécurité FIDO2 MF résistante à l'hameçonnage.

Un mot de passe robuste et bien géré fourni à la PC combiné à une clé de sécurité FIDO2 1F résistante à l'hameçonnage et dotée d'un bouton-poussoir permettant de vérifier la présence physique (utilisé pour s'authentifier auprès de la PC par l'entremise de WebAuthn sur une plateforme informatique distincte) est aussi une solution acceptable mais non préférée, puisqu'un mot de passe doit être envoyé à la PC aux fins de vérification. Toutefois, cette combinaison d'authentifiants constitue une solution préférée pour les utilisateurs ordinaires, comme indiqué ci-dessus.

Veuillez noter que l'utilisation d'authentifiants répondant aux exigences du niveau AAL2/LoA 3 des justificatifs d'identité peut être acceptable pour des administrateurs moins privilégiés, comme un administrateur d'application ou SaaS [46] (sous réserve d'une évaluation du risque). Toutefois, au moins un des authentifiants doit être résistant à l'hameçonnage. Les authentifiants qui satisfont aux exigences du niveau AAL3/LoA 4 des justificatifs d'identité peuvent aussi être utilisés pour satisfaire aux exigences du niveau AAL2/LoA 3 lorsque cela s'avère utile.

Bien que la portée du présent document soit axée sur les exigences techniques, il faut savoir que le choix d'authentifiants appropriés pour un ministère donné dépend de plusieurs facteurs, y compris la capacité de tirer parti des investissements existants, le coût global, l'expérience utilisateur, etc. En fin de compte, l'objectif est de trouver **l'équilibre entre la sécurité, la facilité de gestion, l'interopérabilité, le coût et l'expérience utilisateur afin de déployer des solutions d'AMF appropriées au sein du GC.**

En ce qui concerne l'acquisition d'authentifiants, les ministères sont censés utiliser des solutions, des actifs et des services de TI pangouvernementaux ou partagés afin d'éviter la redondance, lorsqu'ils sont disponibles et appropriés, comme le précise la section 4.4.2.3 de la *Politique sur les services et le numérique*. À cette fin, les ministères peuvent tirer parti des services d'entreprise qui prennent en charge l'AMF, notamment en utilisant les arrangements en matière d'approvisionnement (AMA) établis par Services partagés Canada (SPC).

Enfin, il s'agit d'un domaine complexe en constante évolution, et tant les technologies d'authentification que les menaces qui pèsent sur ces technologies continuent de changer, parfois très rapidement. Les recommandations formulées dans le présent document sont donc susceptibles d'être modifiées au fil du temps. En outre, plusieurs des considérations techniques décrites ci-dessus sont évolutives et pourraient avoir une incidence sur les recommandations à l'avenir, notamment :

- la prise en charge potentielle des clés d'accès synchronisées au niveau AAL2/LoA 3 (voir la section 2.3.7.2);
- le rôle et la viabilité potentiels de l'attestation d'entreprise (voir la section 2.3.7.3);
- l'évolution des conseils en matière d'authentification des utilisateurs, en particulier l'ITSP.30.031 v4 (en cours de rédaction) et la version 4 des

Digital Identity Guidelines du NIST (également en cours de rédaction).

Bien qu'il n'en soit pas question dans le présent document, les renseignements sur la conception et la mise en œuvre des sujets connexes indiqués à la section 2.4 doivent être élaborés, notamment la liaison des authentifiants aux utilisateurs individuels, les options de récupération des authentifiants, les solutions globales de contrôle d'accès en fonction du risque et les scénarios PAP.

Pour toute question ou interprétation du présent document, veuillez communiquer avec la Division de la cybersécurité du SCT à l'adresse suivante : zztbscybers@tbs-sct.gc.ca.

4. Références

1. CBC News, Spy agency chief says new powers would help stop cyberattacks before they happen
2. Verizon, 2024 Data Breach Investigations Report
3. CBC News, Cyberattacks targeting CRA, Canadians' COVID-19 benefits have been brought under control: officials
4. Secrétariat du Conseil du Trésor du Canada, *Recommandations pour l'authentification à deux facteurs des utilisateurs dans le domaine opérationnel du gouvernement du Canada*; remplacé par le présent document
5. Conseil du Trésor, *Politique sur les services et le numérique*
6. Conseil du Trésor, *Directive sur les services et le numérique*
7. Conseil du Trésor, *Directive sur la gestion de l'identité – Annexe A : Norme sur l'assurance de l'identité et des justificatifs*
8. Secrétariat du Conseil du Trésor du Canada, *Ligne directrice sur la définition des exigences en matière d'authentification*

9. Secrétariat du Conseil du Trésor du Canada, *Ligne directrice sur l'assurance de l'identité*
10. Centre canadien pour la cybersécurité, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3)*
11. Centre canadien pour la cybersécurité, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v4)*; pas encore disponible (en cours de rédaction)
12. Centre canadien pour la cybersécurité, *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B – ITSP.40.111*
13. Centre canadien pour la cybersécurité, *Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062)*
14. Centre canadien pour la cybersécurité, *Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)*
15. Centre canadien pour la cybersécurité, *Annexe 2 – Activités de gestion des risques liés à la sécurité des systèmes d'information (ITSG-33)*
16. National Institute of Standards and Technology (NIST) des États-Unis, *Digital Identity Guidelines: Revision 3* (NIST SP 800-63-3 Series)
17. National Institute of Standards and Technology (NIST) des États-Unis, *Digital Identity Guidelines*Initial Public Draft, Revision 4 (NIST SP 800-63-4 Series)
18. National Institute of Standards and Technology (NIST) des États-Unis, *Zero Trust Architecture* (NIST SP 800-207)
19. W3C, *Web Authentication: An API for Accessing Public Key Credentials – Level 2*
20. FIDO Alliance, *User Authentication Specifications Overview*
21. FIDO Alliance, Client-*to-Authenticator Protocol*
22. Gartner, *Zero Trust is an Initial Step on the Roadmap to CARTA*; accessible par abonnement à Gartner

23. Gartner, *Guidance for Selecting User Authentication Solutions*; accessible par abonnement à Gartner

5. Termes clés

Les termes clés utilisés dans le présent document sont définis ci-dessous. Les définitions sont copiées ou tirées des sources indiquées dans la troisième colonne. Des précisions ont été ajoutées entre crochets à certaines définitions.

Terme	**Définition**	**Source**
Activation	Processus consistant à saisir un **facteur d'activation** dans un **authentifiant multifactoriel** pour permettre son utilisation pour l'**authentification**.	NIST SP 800-63-4

Terme	Définition	Source
Appareil mobile	Dispositif informatique portable de petite taille pouvant être facilement transporté par une seule personne. Ce type de dispositif est conçu pour fonctionner sans connexion physique (p. ex., émettre ou recevoir des données sans fil), possède une capacité de stockage de données locale et inamovible, et est alimenté pendant de longues périodes par une source d'énergie autonome. Les appareils mobiles peuvent également être dotés de capacités de communication vocale, de capteurs intégrés qui permettent de capturer de l'information (p. ex., photographier, filmer, enregistrer ou localiser), ou de fonctions intégrées de synchronisation des données locales avec des emplacements à distance. Les exemples incluent les téléphones intelligents, les tablettes et les liseuses électroniques. [Dans le présent document, les références aux appareils mobiles désignent généralement un téléphone intelligent, mais il existe des cas d'utilisation limités où le dispositif pourrait être un téléphone cellulaire de base (p. ex., les téléphones cellulaires de base peuvent prendre en charge la messagerie textuelle, mais ils n'ont pas les fonctionnalités sophistiquées d'un téléphone intelligent, notamment la capacité d'héberger et d'exécuter des applications mobiles). Notez que le terme « téléphone intelligent » est également utilisé dans le présent document, notamment dans le contexte d'exemples ou de cas d'utilisation particuliers.]	NIST SP 800-53-5 Également mentionné dans la NIST SP 800-124r2

Terme	Définition	Source
Attaque par réinsertion	Tentative d'authentification par la réinsertion d'un message d'authentification antérieur enregistré.	NIST SP 800-63B (section 5.2.8)
Authentifiant	Quelque chose que l'utilisateur possède et contrôle (généralement un module cryptographique ou un mot de passe) et qui sert à authentifier l'identité de l'utilisateur. Voir également la définition de **justificatif**.	NIST SP 800-63-3
Authentifiant de plateforme	Voir la définition à l'annexe B.	FIDO Alliance
Authentifiant indépendant de la plateforme	Terme générique désignant un authentifiant physiquement séparé (ou amovible) de la plateforme informatique sur laquelle l'authentification de l'utilisateur est réalisée. Les authentifiants itinérants FIDO2 et les cartes à puce basées sur l'ICP en sont des exemples.	Terme générique dérivé de la définition de l'authentifiant itinérant de FIDO et antithèse de la définition de l'authentifiant de plateforme de FIDO
Authentifiant itinérant	Authentifiant FIDO compatible avec n'importe quel dispositif à partir duquel l'utilisateur essaie de se connecter. Les authentifiants itinérants se connectent aux dispositifs des utilisateurs au moyen d'un protocole de transport comme USB, NFC ou Bluetooth. On les désigne souvent par le terme « clés de sécurité ». Un téléphone intelligent peut également servir d'authentifiant itinérant à l'aide de l'authentification inter-appareils de FIDO.	Passkeys.dev Terms: Roaming authenticator

Terme	Définition	Source
Authentifiant lié à une plateforme	Terme générique désignant un authentifiant attaché physiquement en permanence à la plateforme informatique sur laquelle l'authentification de l'utilisateur est réalisée. Il peut s'agir par exemple d'un TPM discret ou d'un ES intégré. Voir aussi la définition de **composant de sécurité matériel intégré**.	Terme générique dérivé de la définition de l'authentifiant de plateforme de FIDO et antithèse de la définition de l'authentifiant itinérant de FIDO
Authentifiant logiciel	Authentifiant qui consiste en un ou plusieurs composants logiciels mis en œuvre dans l'environnement informatique général d'un dispositif d'utilisateur (p. ex., ordinateur portatif ou téléphone intelligent). Les authentifiants logiciels sont caractérisés par les mécanismes de séparation des processus du système d'exploitation. Les authentifiants logiciels peuvent tirer parti de **composants de sécurité matériels intégrés** ou d'un **environnement d'exécution de confiance (EEC)** pour renforcer la limite d'authentifiant logique ou pour conserver les secrets de l'authentifiant. Les authentifiants logiciels sont capables d'obtenir la validation FIPS 140 de niveau 1.	ITSP.30.031 v4

Terme	Définition	Source
Authentifiant matériel	Composant matériel conçu dans un but précis, physiquement séparé de l'environnement informatique général d'un dispositif d'utilisateur. Les authentifiants matériels se caractérisent par une limite physique (boîtier du dispositif, contenant), disposent de ressources de traitement et de stockage dédiées et communiquent avec l'environnement informatique général d'un dispositif d'utilisateur par l'entremise d'une interface physique et d'un protocole définis. Les authentifiants matériels peuvent être complètement séparés du dispositif de l'utilisateur (p. ex., une carte à puce), ou être intégrés dans le dispositif de l'utilisateur (p. ex., module de plateforme sécurisée ou ES). Les authentifiants matériels sont capables d'obtenir la validation FIPS 140 de niveau 3 pour la sécurité physique.	ITSP.30.031 v4
Authentifiant multifactoriel (MF)	Authentifiant qui fournit plus d'un facteur d'authentification distinct, comme un authentifiant cryptographique matériel avec un capteur biométrique intégré nécessaire pour activer l'authentifiant (ou qui nécessite un mot de passe ou un NIP pour activer l'authentifiant). [Le facteur d'authentification utilisé pour déverrouiller ou activer l'authentifiant MF est appelé **facteur d'activation**.]	NIST SP 800-63-3

Terme	Définition	Source
Authentification	Vérification de l’identité d’un utilisateur, d’un processus ou d’un dispositif, souvent comme condition préalable à l’autorisation d’accès aux ressources d’un système.	NIST SP 800-63-3
Authentification multifactorielle (AMF)	Authentification nécessitant au moins deux facteurs d’authentification distincts. L’AMF peut être réalisée à l’aide d’un authentifiant multifactoriel ou d’une combinaison d’authentifiants appropriés qui fournissent différents facteurs d’authentification. [Les expressions AMF et authentification à deux facteurs (A2F) sont parfois utilisées de manière interchangeable, mais en fait, elles ne sont pas toujours synonymes. L’A2F signifie l’utilisation d’exactement deux facteurs d’authentification alors que l’AMF signifie l’utilisation d’au moins deux facteurs d’authentification.]	NIST SP 800-63-3

Terme	Définition	Source
Clé d’accès Voir également les entrées « Clé d’accès synchronisée » et « Clé d’accès liée à un appareil »	Terme général, centré sur l’utilisateur final, qui désigne un justificatif FIDO2 ou WebAuthn détectable. À l’instar du terme « mot de passe », le terme courant « clé d’accès » s’emploie dans les conversations et les expériences de tous les jours (on dit, « une clé d’accès » ou « des clés d’accès »). Les clés d’accès sont conçues pour simplifier la procédure de connexion. Toutes les clés d’accès peuvent offrir une expérience d’ouverture de session moderne, par exemple, avec une interface utilisateur à remplissage automatique ou un bouton « Se connecter avec une clé d’accès ». D’un point de vue technique, il existe deux types de clés d’accès : synchronisées et liées à un appareil. [Les clés d’accès sont des justificatifs d’identité détectables, et la dernière version préliminaire de WebAuthn Level 3 du W3C utilise ces termes comme des synonymes.]	Passkeys.dev Terms: Passkey WebAuthn Level 3 W3C Working Draft
Clé d’accès liée à un appareil	Justificatif FIDO2 détectable lié à un seul authentifiant. Par exemple, les clés de sécurité FIDO2 contiennent généralement des clés d’accès liées à un appareil, puisque le justificatif ne peut pas quitter ce dernier. Les clés d’accès liées à un appareil étaient anciennement appelées **clés d’accès mono-appareils**.	Passkeys.dev Terms – Device-bound passkey

Terme	Définition	Source
Clé d’accès synchronisée	Justificatif FIDO2 détectable et fiable permettant de se connecter sans autre forme d’authentification, comme un mot de passe à usage multiple ou unique. Par fiable, on entend que l’utilisateur peut se servir de la clé d’accès où et quand il en a besoin pour se connecter. Une telle disponibilité s’obtient par différents moyens. Par exemple, les fournisseurs de clés d’accès peuvent synchroniser celles-ci en temps réel entre les appareils d’un utilisateur, les restaurer à partir d’une sauvegarde chaque fois qu’un utilisateur configure un nouvel appareil, les offrir dans différents contextes (une clé établie à partir d’une application peut servir dans le navigateur lorsque l’utilisateur visite le site Web de l’application) ou permettre à l’utilisateur d’appliquer la clé d’accès entre différents appareils en utilisant par exemple la clé d’un téléphone à proximité pour se connecter à partir d’un ordinateur portatif.	Passkeys.dev Terms – Synced passkey
Clé de sécurité FIDO2	**Authentifiant matériel** conforme aux spécifications ou recommandations FIDO2.	

Terme	Définition	Source
Composant de sécurité matériel intégré	Composant matériel contenu dans un point terminal (p. ex., plateforme informatique ou téléphone intelligent) qui fournit un ou plusieurs services de sécurité dédiés. Les composants de sécurité matériels intégrés sont séparés et distincts de l'environnement informatique général (c'est-à-dire de l'unité centrale de traitement principale) à l'intérieur du terminal. Ils sont caractérisés par des ressources de traitement et de mémoire dédiées, ont un périmètre physique défini et communiquent avec d'autres composants de points terminaux au moyen d'une interface et d'un protocole définis. Selon leur mise en œuvre, ces composants peuvent être capables d'obtenir la validation FIPS 140 au niveau 2 (ou plus) pour la sécurité globale et au niveau 3 (ou plus) pour la sécurité physique. Il peut s'agir par exemple d'un TPM discret ou d'un ES intégré.	ITSP.30.031 v4
Contrôle d'accès (logique)	Processus consistant à accorder ou à refuser les demandes reçues pour obtenir et utiliser des renseignements et des services de traitement de renseignements connexes. [Une décision de contrôle d'accès peut être fondée sur de multiples intrants, paramètres et données télémétriques; l'authentification de l'utilisateur n'est qu'une facette du processus]	NIST Computer Security Resource Center Glossary Voir la section 2.4.6 du présent document

Terme	Définition	Source
Élément sécurisé (ES)	Composant matériel sécurisé et inviolable utilisé dans un dispositif pour offrir la sécurité, la confidentialité et l’environnement d’applications multiples requis par divers modèles opérationnels. Peut exister sous n’importe quel facteur de forme : ES embarqué ou intégré, SIM, carte à puce, carte microSD intelligente, etc.	GlobalPlatform Technology: Root of Trust Definitions and Requirements – Version 1.1

Terme	Définition	Source
Environnement d’exécution de confiance (EEC)	Espace sécurisé du processeur principal d’un dispositif connecté qui garantit que les données de nature sensible sont conservées, traitées et protégées dans un environnement isolé et fiable. Il offre donc une protection contre les attaques logicielles générées dans le système d’exploitation riche. La capacité de l’EEC à garantir l’exécution sûre des logiciels de sécurité autorisés, connus sous le nom d’applications de confiance, lui permet d’assurer une sécurité de bout en bout. En effet, il protège l’exécution du code authentifié, la confidentialité, l’authenticité, le respect de la vie privée, l’intégrité du système et les droits d’accès aux données. Comparativement aux autres environnements de sécurité sur le dispositif, l’EEC offre également des vitesses de traitement élevées et une grande quantité de mémoire accessible. L’objectif principal de l’environnement d’exécution isolé, fourni par l’EEC, est de protéger le dispositif et les applications de confiance. Approche selon laquelle des modes d’exécution supplémentaires sont introduits dans une unité centrale de traitement afin de permettre un traitement fiable. La limite de l’authentifiant est obtenue par une séparation à la fois temporelle et physique sur la même unité centrale de traitement que celle utilisée pour l’informatique générale. Le degré d’isolation des ressources dépend de la mise en œuvre de la technologie.	Introduction to Trusted Execution Environments ITSP.30.031 v4

Terme	Définition	Source
Facteur d’activation	**Facteur d’authentification** supplémentaire utilisé pour permettre une **authentification** réussie avec un **authentifiant multifactoriel**. Comme tous les authentifiants multifactoriels sont des authentifiants matériels physiques, les facteurs d’activation sont soit des secrets mémorisés, soit des facteurs biométriques. [Quelque chose que l’utilisateur saisit (mot de passe, NIP, etc.) ou présente (données biométriques) pour déverrouiller un authentifiant multifactoriel]	NIST SP 800-63-4
Facteur d’authentification	Les trois types de facteurs d’authentification sont quelque chose que vous connaissez, quelque chose que vous possédez, et quelque chose que vous produisez ou qui vous caractérise. Chaque authentifiant possède un ou plusieurs facteurs d’authentification.	NIST SP 800-63-3
Interception (attaque de l’intercepteur)	Attaque par laquelle l’auteur de la menace s’immisce entre deux parties communicantes légitimes afin d’intercepter ou de modifier les données qui circulent entre elles. Dans le contexte de l’authentification, l’auteur de la menace s’immisce entre l’utilisateur et le vérificateur, entre l’utilisateur et le fournisseur de justificatifs d’identité (FJI) au moment de l’inscription, ou entre l’utilisateur et le FJI au moment de la liaison de l’authentifiant. [Anciennement appelé « attaquant du milieu » et également appelé « attaque de l’intercepteur ».]	NIST SP 800-63-3 NIST SP 800-63B-4 (Revision 4, Initial Public Draft)

Terme	Définition	Source
Justificatif d’identité	Objet ou structure de données qui lie légitimement une identité, au moyen d’un ou de plusieurs identifiants et (facultativement) d’autres attributs, à au moins un authentifiant détenu et contrôlé par un utilisateur. [Les termes « justificatif » et « authentifiant » sont parfois utilisés de manière interchangeable; il s’agit de termes connexes mais différents. Un authentifiant, comme défini ci-dessus, est utilisé conjointement avec un justificatif d’identité afin d’authentifier un utilisateur. Un exemple classique est le chiffrement asymétrique, où l’authentifiant utilise une clé de signature privée exclusive à l’utilisateur pour signer numériquement des données (généralement un nonce et d’autres données dans un protocole simulation-réponse) et où le certificat de clé publique de l’utilisateur est le justificatif utilisé par la PC pour vérifier la signature numérique.]	NIST SP 800-63-3
Module de plateforme sécurisée (TPM)	De nombreuses définitions publiées suggèrent qu’un TPM est une puce en silicium autonome qui est fixée à la carte mère d’une plateforme informatique et qui est dédiée à des fonctions de sécurité comme les opérations cryptographiques et le stockage des clés. Cette description s’applique bien à un type de TPM (appelé « TPM discret » par le Trusted Computing Group), mais il existe en réalité différents types de TPM, comme expliqué à l’annexe C.	Voir l’annexe C.

Terme	Définition	Source
Niveau d’assurance (LoA) des justificatifs	Niveau de confiance requis pour assurer qu’une personne a gardé le contrôle des justificatifs qui lui ont été confiés et que ceux-ci n’ont pas été compromis. Il existe quatre niveaux de confiance définis comme suit : • LoA 4 : confiance très élevée • LoA 3 : confiance élevée • LoA 2 : confiance moyenne • LoA 1 : confiance faible	Norme sur l’assurance de l’identité et des justificatifs
Nonce (ou valeur de défi)	Valeur aléatoire ou non répétée qui est incluse dans les données échangées par un protocole [d’authentification], généralement dans le but d’assurer la transmission de données en direct plutôt que de données réinsérées, ce qui permet de détecter les attaques par réinsertion et de s’en prémunir.	NIST Computer Security Resource Center: Glossary
Partie de confiance (PC) (ou partie utilisatrice)	Entité qui se fie aux authentifiants et aux justificatifs d’identité de l’utilisateur ou sur l’évaluation du vérificateur de l’identité d’une personne, généralement pour traiter une transaction ou accorder l’accès aux renseignements ou à un système.	NIST SP 800-63-3
Résistance à l’hameçonnage	Capacité du protocole d’authentification de détecter les secrets d’authentification et les résultats valides de l’authentifiant et d’empêcher leur divulgation à une fausse partie de confiance, indépendamment du niveau de vigilance de l’abonné.	NIST SP 800-63B-4 (Revision 4, Initial Public Draft) (Section 5.2.5)

Terme	Définition	Source
Vérificateur	Entité qui vérifie l’identité de l’utilisateur en s’assurant qu’il possède et contrôle un ou deux authentifiants au moyen d’un protocole d’authentification.	NIST SP 800-63-3

6. Sigles et abréviations

1F	À un facteur
AAL	Niveau d’assurance des authentifiants
AC	Application de confiance
AitM	Attaque de l’intercepteur
AMF	Authentification multifactorielle
API	Interface de programmation d’applications
ARC	Agence du revenu du Canada
CBC	Canadian Broadcasting Corporation
CTAP 2.2	Spécification Client to Authenticator Protocol 2.2 de FIDO
EEC	Environnement d’exécution de confiance
ES	Élément sécurisé
FIDO	Fast Identity Online
FIPS 140	Federal Information Processing Standard 140
FJI	Fournisseur de justificatifs d’identité
GC	Gouvernement du Canada
GIJIA	Gestion de l’identité, des justificatifs d’identité et de l’accès
HB	Hors bande
ICP	Infrastructure à clés publiques
ITSAP	Programme de sensibilisation à la sécurité de la TI

1F	À un facteur
ITSP	Programme de la sécurité de la TI
IU à remplissage automatique	Interface utilisateur
LoA	Niveau d’assurance
MF	Multifactoriel
microSD	Carte microSD (« secure digital »)
MitM	Intercepteur
MPU	Mot de passe à usage unique
MS	Microsoft
NFC	Communication en champ proche
NIP	Numéro d’identification personnel
NIST	National Institute of Standards and Technology
PAP	Prenez vos authentifiants personnels
PC	Partie de confiance
RSA	RSA Security (rsa.com)
SaaS	Logiciel-service
SAML	Langage de balisage des assertions de sécurité
SCT	Secrétariat du Conseil du Trésor du Canada
SIM	Module d’identification de l’abonné
SMS	Service de messagerie texte
SP	Publication spéciale
SS7	Protocole SS7
TI	Technologie de l’information
TLS	Sécurité de la couche transport
TPM	Module de plateforme sécurisée
VIP	Vérification de l’identité personnelle

1F	À un facteur
W3C	World Wide Web Consortium
WebAuthn	Web Authentication: An API for Accessing Public Key Credentials: Level 2
WHfB	Windows Hello for Business

Annexe A : Survol et comparaison des niveaux d’assurance

▶ In this section

A-1 Introduction

La présente annexe a pour objet de présenter une vue d’ensemble du modèle à quatre niveaux d’assurance actuellement utilisé par le gouvernement du Canada (GC) et de comparer ce modèle aux *Digital Identity Guidelines* (version 3) du National Institute of Standards and Technology (NIST) des États-Unis [en anglais seulement].

A-2 Niveaux d’assurance du GC

Le degré de confiance à l’égard de l’identité, des justificatifs et de l’authentification au sein du GC s’exprime sous forme de niveaux d’assurance (LoA) fondés sur un modèle à quatre niveaux, où le LoA 1 est le niveau plus faible et le LoA 4, le niveau le plus élevé. Ce modèle est conforme à la norme ISO/IEC 29115 et, jusqu’en juin 2017, cadrait avec le guide sur l’authentification des utilisateurs publié par le NIST (voir la section Lien avec le guide sur l’authentification des utilisateurs du NIST ci-dessous pour en savoir plus).

Le GC a élaboré plusieurs instruments de politique et documents d'orientation qui contiennent les définitions et les exigences associées à chaque niveau d'assurance, notamment les suivants :

- *Directive sur la gestion de l'identité – Annexe A : Norme sur l'assurance de l'identité et des justificatifs* : définit les quatre niveaux d'assurance liés à l'assurance de l'identité et à l'assurance des justificatifs.
- *Ligne directrice sur la définition des exigences en matière d'authentification* : décrit la méthode utilisée pour déterminer le niveau d'assurance minimal requis pour l'authentification des utilisateurs dans un contexte donné.
- *Ligne directrice sur l'assurance de l'identité* : précise les exigences minimales permettant d'établir l'identité d'une personne pour un niveau d'assurance donné.
- *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3)* : fournit des conseils techniques sur les exigences en matière d'authentification des utilisateurs à chaque niveau d'assurance.

Il est à noter que le GC fait la distinction entre assurance de l'identité et assurance des justificatifs. La *Norme sur l'assurance de l'identité et des justificatifs* (publiée le 1er juillet 2019) établit les quatre niveaux d'assurance associés à l'identité et aux justificatifs, qui sont indiqués dans les tableaux suivants.

Tableau A1 : Assurance de l'identité

Niveau d'assurance	Description
4	Besoin d'un **niveau très élevé de confiance** que la personne est celle qu'elle affirme être.

Niveau d’assurance	Description
3	Besoin d’un **niveau élevé de confiance** que la personne est celle qu’elle affirme être.
2	Besoin d’un **certain niveau de confiance** que la personne est celle qu’elle affirme être.
1	Besoin d’un **faible niveau de confiance** que la personne est celle qu’elle affirme être.

Tableau A2 : Assurance des justificatifs

Niveau d’assurance	Description
4	Besoin d’un **niveau très élevé de confiance** que la personne a gardé le contrôle des justificatifs qui lui ont été confiés et que ceux-ci n’ont pas été compromis.
3	Besoin d’un **niveau élevé de confiance** que la personne a gardé le contrôle des justificatifs qui lui ont été confiés et que ceux-ci n’ont pas été compromis.
2	Besoin d’un **certain niveau de confiance** que la personne a gardé le contrôle des justificatifs qui lui ont été confiés et que ceux-ci n’ont pas été compromis.
1	Besoin d’un **faible niveau de confiance** que la personne a gardé le contrôle des justificatifs qui lui ont été confiés et que ceux-ci n’ont pas été compromis.

La version du 1er juillet 2019 de la *Norme sur l’assurance de l’identité et des justificatifs* remplace la version désormais archivée, qui a été publiée le 1er février 2013. Les définitions des niveaux d’assurance de la version originale du 1er février 2013 comprenaient la notion de préjudice, ce qui n’est pas le cas dans la version mise à jour [47]. Cependant, les anciennes

définitions sont reprises dans la *Ligne directrice sur la définition des exigences en matière d'authentification*, qui a été publiée le 30 novembre 2012 et n'a pas été mise à jour depuis.

La *Ligne directrice sur la définition des exigences en matière d'authentification* décrit un processus indépendant de la technologie mis à la disposition des propriétaires d'entreprise pour déterminer le niveau minimal d'assurance de l'authentification requis pour atteindre les objectifs d'un programme, fournir un service ou exécuter correctement une transaction. Une fois qu'ils ont déterminé le niveau d'assurance minimal, ils peuvent consulter les sources appropriées pour connaître les exigences à respecter pour atteindre ce niveau d'assurance. Plus précisément, la *Ligne directrice sur l'assurance de l'identité* énonce les exigences en matière d'assurance de l'identité à chaque LoA, et le *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3)* traite des exigences en matière d'assurance des justificatifs et des exigences liées au processus d'authentification connexe.

Comme le précise le document ITSP.30.031 v3, le niveau d'assurance global de l'authentification correspond au niveau d'assurance le plus bas associé à chacun des domaines suivants :

- confirmation de l'identité, enregistrement et processus d'émission;
- exigences visant les authentifiants [48];
- gestion des authentifiants et des justificatifs;
- protocole d'authentification;
- exigences en matière d'assertion ou de fédération;
- journalisation des événements;
- assurance de la sécurité.

Par exemple, si on détermine que le niveau d'assurance global de l'authentification doit être LoA 3, tous ces domaines doivent respecter les exigences établies pour le niveau 3 ou le niveau 4 [49]. Si l'un de ces

domaines est de niveau 2 seulement, le niveau d’assurance de l’authentification correspondra au LoA 2, même si les autres domaines sont de niveau 3 ou 4. La figure A1 et la figure A2 illustrent cet exemple.

Tableau A1 : Niveau d’assurance global – exemple 1

Confirmation de l’identité, enregistrement et processus d’émission	1	2	3	4
Exigences visant les authentifiants	1	2	3	4
Gestion des authentifiants et des justificatifs	1	2	3	4
Processus ou protocole d’authentification	1	2	3	4
Assertions ou fédération	1	2	3	4
Journalisation des événements	1	2	3	4
Assurance de la sécurité	1	2	3	4
Niveau d’assurance global de l’authentification		2		

▶ Tableau A1 - version textuelle

Tableau A2 : Niveau d’assurance global – exemple 2

Confirmation de l’identité, enregistrement et processus d’émission	1	2	3	4
Exigences visant les authentifiants	1	2	3	4
Gestion des authentifiants et des justificatifs	1	2	3	4
Processus ou protocole d’authentification	1	2	3	4
Assertions ou fédération	1	2	3	4
Journalisation des événements	1	2	3	4
Assurance de la sécurité	1	2	3	4
Niveau d’assurance global de l’authentification			3	

▶ Tableau A2 - version textuelle

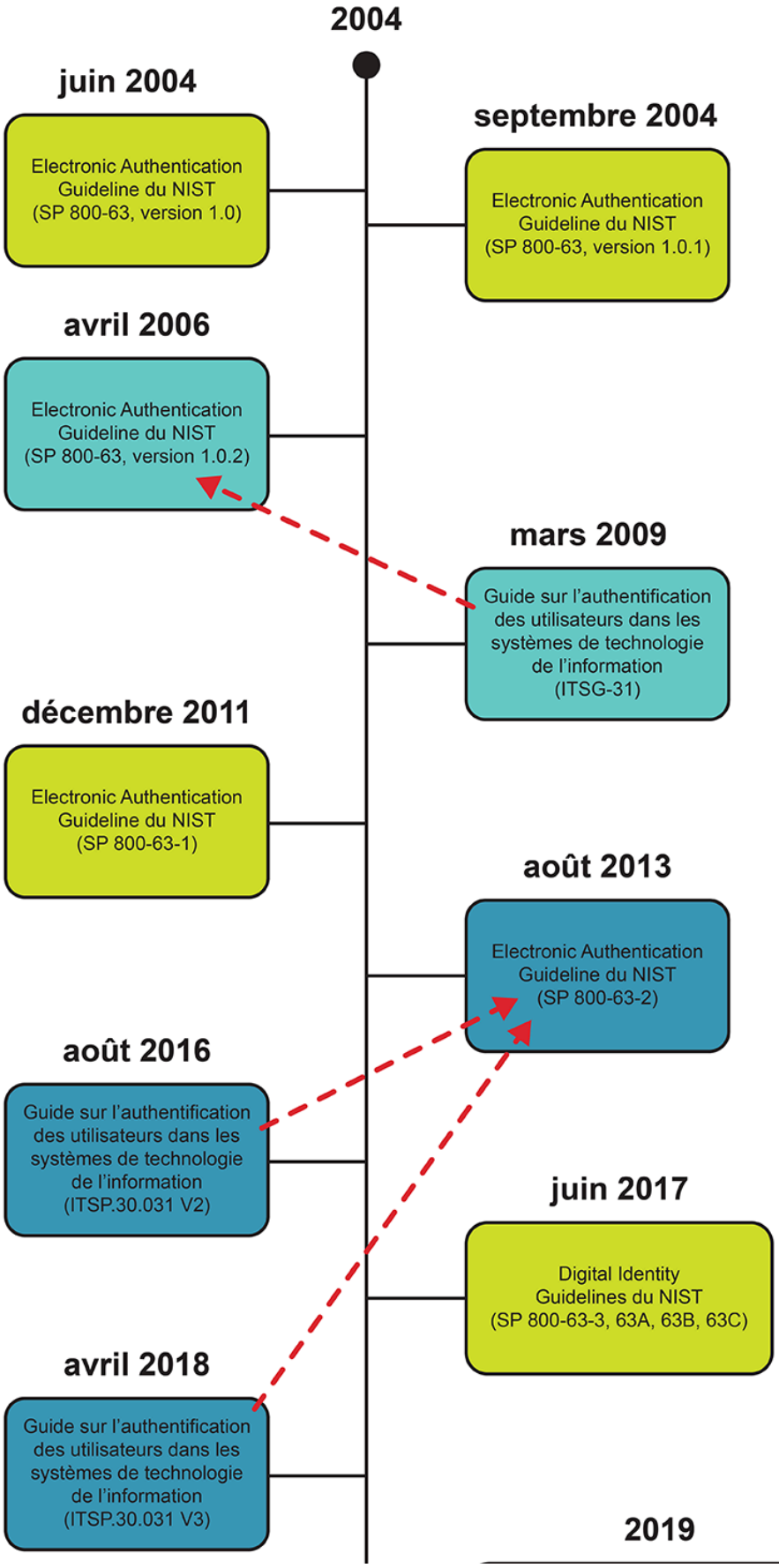
Comme il a été mentionné précédemment, les exigences de chaque LoA associé à la confirmation de l'identité, à l'enregistrement et au processus d'émission sont énoncées dans la *Ligne directrice sur l'assurance de l'identité*, et les exigences de chaque LoA applicables à tous les autres domaines sont décrites dans le document ITSP.30.031 v3.

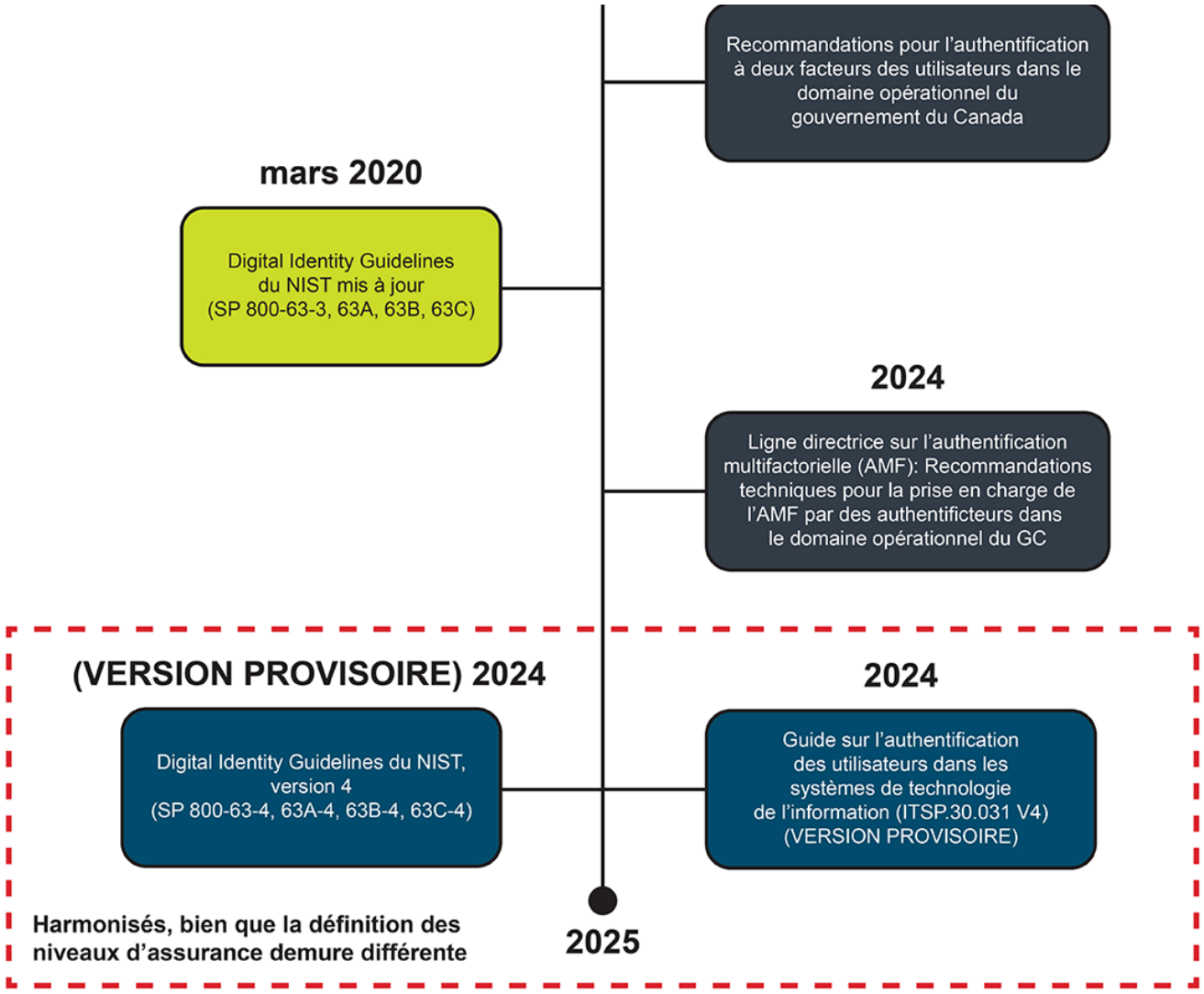
A-3 Lien avec le guide sur l'authentification des utilisateurs du NIST

Le NIST des États-Unis a publié son premier guide sur l'authentification des utilisateurs en 2004. Ce guide reposait sur les quatre niveaux d'assurance établis dans le document OMB M-04-04 du White House Office of Management and Budget des États-Unis. Le guide sur l'authentification des utilisateurs, appelé *Electronic Authentication Guideline*, a évolué au fil des versions, comme l'illustre la figure A3. Le Centre de la sécurité des télécommunications (CST) et le Centre canadien pour la cybersécurité (CCC) ont aussi publié un guide sur l'authentification des utilisateurs, comme le montre la figure A3 (les flèches pointillées indiquent la version des lignes directrices du NIST qui a servi de référence).

Figure A3 : Évolution des guides sur l'authentification des utilisateurs du NIST et du CST et du CCC

Évolution des guides techniques sur l'authentification des utilisateurs des États-Unis et du GC





▶ Figure A3 - version textuelle

- les sections 1 à 4 du document SP 800-63-2 sont remplacées par le document SP 800-63-3 [en anglais seulement];
- la section 5 du document SP 800-63-2 est remplacée par le document SP 800-63A [en anglais seulement];
- les sections 6 à 8 du document SP 800-63-2 sont remplacées par le document SP 800-63B [en anglais seulement];
- la section 9 du document SP 800-63-2 est remplacée par le document SP 800-63C [en anglais seulement].

La différence la plus marquante est sans doute que le nouveau document *Digital Identity Guidelines* du NIST ne repose plus sur les quatre niveaux d'assurance [50], mais plutôt sur trois niveaux d'assurance définis pour trois

domaines différents : identité, authentification et authentifiants, et fédération. Autrement dit, le nouveau document définit un niveau d'assurance explicite pour chacun de ces trois domaines, au lieu d'exprimer le niveau global d'assurance de l'authentification avec une seule valeur. Les instruments de politique du GC et les mises en œuvre techniques connexes sont toutefois toujours fondés sur les quatre niveaux d'assurance initiaux. Il reste à voir si, ou quand, cela changera. Il est donc important de comprendre les liens entre les deux différents modèles.

Le tableau A3 présente les trois niveaux d'assurance de chaque domaine défini dans la version 3 des *Digital Identity Guidelines* [51] du NIST et les associe aux niveaux d'assurance équivalents (ou approximatifs) du GC. Comme il n'y a pas toujours d'équivalence absolue, certaines correspondances sont approximatives et peuvent comprendre plus d'un niveau. Il importe de noter que les niveaux d'assertion de fédération équivalents du GC sont tirés de la section 7 du document ITSP.30.031 v3.

Tableau A3 : Mises en correspondance des niveaux d'assurance

Niveaux d'assurance du document SP 800-63-3 du NIST		**Équivalents du GC**
Niveau d'assurance de l'identité (IAL)		
IAL1	Il n'est pas nécessaire de lier le demandeur à une identité réelle précise. Tous les attributs fournis dans le cadre du processus d'authentification sont attestés d'emblée ou doivent être considérés comme tel (y compris les attributs qu'un fournisseur de justificatifs d'identité [FJI] assigne à une partie de confiance [PC]).	**LoA de l'identité 1**
IAL2	La preuve confirme l'existence réelle de l'identité alléguée et atteste que le demandeur est bien associé à cette identité dans le monde réel. L'IAL2 introduit l'obligation de confirmer l'identité à distance ou en personne. Les FJI peuvent confirmer les attributs de PC pour permettre l'utilisation d'un pseudonyme avec des attributs vérifiés.	**LoA de l'identité 2 et 3** [52]

Niveaux d’assurance du document SP 800-63-3 du NIST		Équivalents du GC
IAL3	La confirmation de l’identité doit être effectuée en personne. Un représentant autorisé et formé du FJI doit vérifier les attributs d’identité. Comme pour l’IAL2, les FJI peuvent confirmer les attributs de PC pour permettre l’utilisation d’un pseudonyme avec des attributs vérifiés.	**LoA de l’identité 4**
Niveau d’assurance des authentifiants (AAL)		
AAL1	L’AAL1 garantit dans une certaine mesure que le demandeur contrôle un authentifiant lié au compte de l’abonné. L’AAL1 nécessite une authentification à facteur unique ou à facteurs multiples faisant appel à un large éventail de technologies d’authentification disponibles. Une authentification réussie exige que le demandeur prouve qu’il possède et contrôle l’authentifiant au moyen d’un protocole d’authentification sécurisé.	**LoA des justificatifs 2**
AAL2	L’AAL2 fournit un niveau de confiance élevé quant au fait que le demandeur contrôle les authentifiants liés au compte de l’abonné. Le demandeur doit prouver qu’il possède et contrôle deux facteurs d’authentification distincts au moyen d’un ou de plusieurs protocoles d’authentification sécurisés. Des techniques cryptographiques approuvées sont requises à partir de l’AAL2.	**LoA des justificatifs 3**
AAL3	L’AAL3 fournit un niveau de confiance très élevé quant au fait que le demandeur contrôle les authentifiants liés au compte de l’abonné. L’authentification à l’AAL3 repose sur la preuve de possession d’une clé au moyen d’un protocole cryptographique. L’authentification à l’AAL3 **doit** faire appel à un authentifiant matériel et un authentifiant offrant une protection contre l’usurpation d’identité du vérificateur; il est **possible** d’utiliser le même appareil pour répondre à ces deux exigences. Pour s’authentifier à l’AAL3, le demandeur **doit** prouver qu’il possède et contrôle deux facteurs d’authentification distincts au moyen d’un ou de plusieurs protocoles d’authentification sécurisés. Des techniques cryptographiques approuvées sont requises.	**LoA des justificatifs 4**

Niveaux d’assurance du document SP 800-63-3 du NIST		Équivalents du GC
Niveau d’assurance de la fédération (FAL) [53]		
FAL1 [54]	Permet à l’abonné d’autoriser la PC à recevoir une assertion du porteur. L’assertion est signée par le fournisseur d’identité au moyen d’une technique cryptographique approuvée.	**LoA de l’assertion 1**
FAL2 [55]	Ajoute l’exigence de chiffrer l’assertion au moyen d’une technique cryptographique approuvée, de sorte que seule la PC puisse la déchiffrer.	**LoA de l’assertion 2**
FAL3	Exige que l’abonné présente une preuve de possession d’une clé cryptographique [56] mentionnée dans l’assertion en plus de l’artéfact d’assertion lui-même. L’assertion est signée par le fournisseur d’identité et chiffrée à l’intention de la PC au moyen d’une technique cryptographique approuvée.	**LoA de l’assertion 4**

A-4 Résumé

Le présent document donne une vue d’ensemble du modèle à quatre niveaux d’assurance du GC et montre comment ces quatre niveaux d’assurance correspondent aux niveaux d’assurance IAL, AAL et FAL des *Digital Identity Guidelines* du NIST. Ces correspondances sont fondées sur la version 3 des *Digital Identity Guidelines* du NIST. On reconnaît toutefois que la version 4 du document, qui est en cours d’élaboration, pourrait avoir d’importantes répercussions sur certaines définitions et correspondances actuelles. Le présent document sera mis à jour en fonction des changements une fois que la version 4 sera officiellement publiée en remplacement de la version 3.

Annexe B : Aperçu de Fast Identity

Online (FIDO)

▶ In this section

B-1 Introduction

« Fast Identity Online Alliance, ou plus simplement FIDO Alliance, est un consortium public-privé multi-intervenants composé de plus de 250 entreprises et agences gouvernementales du monde entier et dont la mission consiste à élaborer des normes et des programmes de certification pour l'authentification multifactorielle (AMF) et sans mot de passe et la vérification d'identité à distance [57]. » [traduction]

La page Web User Authentication Specifications Overview de FIDO Alliance donne un aperçu des spécifications d'authentification des utilisateurs, dont la description détaillée peut être téléchargée sur la page Web Download Authentication Specifications. Ces spécifications et les liens entre chacune peuvent s'avérer quelque peu déroutants de prime abord. C'est pourquoi le présent aperçu aide à mieux s'orienter dans le paysage des spécifications techniques de FIDO Alliance (et du W3C) et à cerner quelques-uns des facteurs techniques les plus pertinents dans le contexte opérationnel du GC.

Bien que la présente vue d'ensemble porte essentiellement sur les spécifications techniques, sachez que la documentation de FIDO Alliance couvre bien plus que cela. Toute personne qui souhaite approfondir le sujet est invitée à explorer le site Web de FIDO Alliance pour se faire une meilleure idée de la documentation disponible, y compris les spécifications techniques, le programme de certification, les exigences en matière de sécurité et les études de cas.

À noter que le contenu du présent aperçu a été puisé dans les informations disponibles au moment de sa rédaction et qu'il peut changer alors que les spécifications techniques et les produits mis en œuvre continuent d'évoluer. Il faut également savoir que certaines des informations disponibles en ligne concernant les détails de la mise en œuvre technique de FIDO Alliance sont parfois contradictoires ou trompeuses. Dans la mesure du possible, l'aperçu désigne les domaines qui affichent de telles lacunes et utilise les spécifications appropriées comme source définitive. En outre, les entreprises ou les produits mentionnés ici ne sont utilisés qu'à titre d'exemple, et cet usage ne doit en aucun cas être vu comme une forme quelconque d'appui à leur égard.

B-2 Aperçu technique

Les authentifiants FIDO utilisent le chiffrement asymétrique pour authentifier l'utilisateur. Chaque fois que l'utilisateur s'enregistre auprès d'une nouvelle partie de confiance (PC) – un site Web, par exemple –, l'authentifiant génère une paire de clés publique-privée différente, qui facilite par la suite l'authentification de l'utilisateur auprès de cette partie (voir Relying Party Identifier (RP ID), *Web Authentication: An API for accessing Public Key Credentials, Level 2*). Chaque paire de clés – parfois appelée « à portée définie » ou « liée à une origine » – est liée à une seule partie de confiance et ne peut donc pas servir à s'authentifier auprès d'une autre. Ces propriétés rendent les authentifiants FIDO à la fois résistants à l'hameçonnage et aux interceptions.

Les authentifiants FIDO peuvent être liés à l'appareil d'un utilisateur – un ordinateur portatif, par exemple. On les appelle alors des **authentifiants de plateforme**. Lorsqu'ils se trouvent sur un dispositif ou un appareil distinct – une clé de sécurité ou un téléphone mobile, par exemple –, on parle plutôt d'**authentifiants itinérants**.

FIDO Alliance a publié les trois séries de spécifications techniques ci-dessous.

1. **Universal Second Factor (U2F).** Ensemble de spécifications de FIDO Alliance qui définissent une solution d'authentification de second facteur, utilisée de concert avec un premier facteur (généralement un nom d'utilisateur ou un mot de passe). Comme indiqué ci-dessous, plusieurs spécifications U2F ont été remplacées, mais les authentifiants U2F sont toujours pris en charge.
2. **Universal Authentication Framework (UAF).** Ensemble de spécifications de FIDO Alliance qui définissent une solution d'authentification multifactorielle sans mot de passe (principalement utilisée comme trousse de développement de logiciels [SDK] avec les applications natives et les modules d'extension biométriques).
3. **Client-to-Authenticator Protocol (CTAP).** Spécification de FIDO Alliance qui décrit un protocole de communication entre les authentifiants itinérants (p. ex., les clés de sécurité FIDO ou les **clés d'accès** d'appareils mobiles) et les navigateurs ou plateformes compatibles avec la norme WebAuthentication, ou WebAuthn, au moyen de différentes technologies de transport, comme USB, NFC et BLE [58]. Notez également que la spécification CTAP 2.1 décrit en réalité deux versions du protocole, soit CTAP1 – ou U2F par le passé – et CTAP2, qui prend en charge l'authentification sans mot de passe, l'authentification de second facteur et l'authentification multifactorielle. Sachez aussi que la spécification CTAP 2.1 remplace le format de message brut U2F, le protocole HID U2F, le protocole NFC U2F et les spécifications Bluetooth U2F [59]. À l'heure actuelle, c'est la version 2.1 de la spécification CTAP qui est en vigueur, la version 2.2 étant en cours d'élaboration (l'ébauche la plus récente au moment de rédiger le présent document est la spécification CTAP 2.2 datée du 21 mars 2023). Notez que la spécification CTAP 2.2 définit un nouveau

transport hybride visant à normaliser le protocole d'utilisation de clés d'accès avec des téléphones intelligents pour s'authentifier auprès de parties de confiance auxquelles on accède depuis un autre appareil (un ordinateur portatif, une tablette, etc.). C'est ce qu'on appelle **l'authentification inter-appareils** (AIA).

En outre, le consortium W3C a publié une spécification complémentaire (en collaboration avec FIDO Alliance), la recommandation W3C intitulée Web Authentication: An API for Accessing Public Key Credentials, ou norme WebAuthn. La norme WebAuthn définit une interface de programmation d'applications (API) Web normalisée et intégrée aux navigateurs et aux plateformes pour permettre la prise en charge de l'authentification FIDO [60]. Elle remplace la spécification de l'API JavaScript U2F, mais demeure rétrocompatible et est dotée de fonctionnalités additionnelles. La rétrocompatibilité avec l'API JavaScript U2F garantit la prise en charge ininterrompue des authentifiants U2F. Notez que tous les principaux navigateurs prennent en charge l'API de la norme WebAuthn (voir la page Web FIDO2: Web Authentication). La version actuelle de la norme WebAuthn recommandée est le niveau 2, le niveau 3 étant en cours d'élaboration (au moment de la rédaction du présent document, l'ébauche la plus récente du niveau 3 est la recommandation Web Authentication: An API for Accessing Public Key Credentials Level 3 datée du 13 mars 2024).

À noter que la nomenclature dans ce domaine tend à varier et peut prêter à confusion. Le terme « FIDO2 » (issu du « projet FIDO2 ») sert essentiellement à désigner collectivement la nouvelle spécification CTAP de FIDO Alliance et la norme WebAuthn recommandée par le W3C. Les spécifications U2F et UAF ne sont pas considérées comme faisant partie de « FIDO2 », bien que cette distinction soit parfois difficile à faire dans diverses publications et divers messages en ligne. En outre, FIDO2 est une extension de la spécification U2F, avec laquelle il est rétrocompatible, et

pourrait éventuellement la remplacer, ce qui ajoute à la confusion. Aux fins du présent document, un « authentifiant FIDO » s'entend au sens le plus large du terme (c'est-à-dire tout authentifiant qui est certifié FIDO). Cela inclut les authentifiants UAF, U2F et FIDO2. Lorsque cela est nécessaire pour fournir davantage de contexte ou de clarté, le type d'authentifiant particulier doit être précisé. En outre, la spécification CTAP et la norme WebAuthn recommandée doivent être désignées séparément lorsque la distinction s'impose.

Voici ce qu'il faut retenir:

- Les authentifiants FIDO sont à la fois résistants à l'hameçonnage et aux interceptions.
- La spécification CTAP décrit comment les authentifiants FIDO externes (c'est-à-dire les authentifiants itinérants physiquement séparés de la plateforme de l'utilisateur) communiquent ou s'interfacent avec les navigateurs et les plateformes compatibles avec la norme WebAuthn recommandée.
- WebAuthn est une API qui permet l'authentification FIDO dans un navigateur Web ou une plateforme.
- Un authentifiant U2F ou CTAP1 sert de deuxième facteur d'authentification de concert avec un premier facteur d'authentification (habituellement, le nom d'utilisateur et le mot de passe).

B-3 Autres renseignements techniques

D'autres renseignements techniques (et des domaines nécessitant une analyse plus approfondie) sont présentés ci-dessous.

B-3.1 Clés d'accès (synchronisées et liées à un appareil)

La signification du terme **clé d'accès** a évolué au cours des dernières années. Certains fournisseurs ont introduit ce terme comme synonyme pour décrire des justificatifs multidispositifs que l'on peut sauvegarder et copier dans plus d'un appareil. En fait, le terme **clé d'accès** s'applique tant aux justificatifs multidispositifs que monodispositifs (voir la page Web FIDO Alliance: Passkeys). Autrement dit, **« clé d'accès** » est un terme générique qui désigne des **justificatifs détectables** FIDO, qu'ils soient multidispositifs (copiables) ou monodispositifs (non copiables). La documentation la plus récente utilise les termes **clé d'accès synchronisée** et **clé d'accès liée à un appareil** (par exemple, voir le document FIDO Deploying Passkeys in the Enterprise: Introduction).

La synchronisation des clés d'accès est une approche qui permet de sauvegarder et de synchroniser (copier) les clés privées utilisées pour authentifier l'utilisateur de plusieurs appareils, ce qui élimine (ou réduit) la nécessité d'enregistrer plusieurs justificatifs auprès d'un même service Web en ligne. Les clés d'accès synchronisées prennent également en charge la synchronisation transparente des justificatifs avec de nouveaux appareils. Cela améliore l'expérience de récupération de l'authentifiant (voir la section Récupération ci-dessous) et permet une authentification transparente des utilisateurs qui utilisent plusieurs appareils pour accéder aux mêmes services Web en ligne. Cependant, il y a des compromis à faire entre l'aspect pratique des clés d'accès synchronisées et les problèmes de sécurité qu'elles pourraient créer.

Le National Institute of Standards and Technology (NIST) des États-Unis a récemment publié de nouvelles directives provisoires sur les authentifiants synchronisés (ou clés d'accès synchronisées). Ces directives provisoires font état des exigences en matière de sécurité à respecter pour que ces authentifiants puissent servir avec le niveau d'assurance (LoA) 3 ou le niveau d'assurance d'authentification (AAL) 2. Cela pourrait bien changer la

donne en améliorant l'expérience utilisateur sans sacrifier la sécurité. Il faut cependant savoir que certains produits ne prennent en charge que les clés d'accès liées à un appareil afin de satisfaire à des exigences d'assurance plus strictes (par exemple, la mise en œuvre de la norme FIDO2 de la série 5 de Yubikey).

Les livres blancs de FIDO Alliance, intitulés FIDO Authentication for Moderate Assurance Use Cases et High Assurance Enterprise FIDO Authentication, apportent des précisions sur les différences entre clé d'accès synchronisée et clé d'accès liée à un appareil en termes d'avantages et d'inconvénients.

B-3.2 Modalité de stockage des justificatifs

Il semble que des renseignements contradictoires (ou trompeurs) soient publiés en ligne au sujet de l'endroit où sont stockées les clés privées servant à authentifier les utilisateurs. Par exemple, le site Web de FIDO Alliance lui-même (voir la page FIDO Authentication) précise textuellement que les justificatifs de connexion FIDO2 chiffrés sont uniques dans chaque site Web, ne quittent jamais l'appareil de l'utilisateur et ne sont jamais stockés sur un serveur. Toutefois, il ressort clairement de la lecture des spécifications de FIDO2 (qui, par définition, font autorité) que les clés de signature privées servant à l'authentification peuvent être stockées sur l'appareil ou sur le serveur (sous forme chiffrée). En particulier, voir les sections 6.2, Authenticator Taxonomy et 6.2.2, Credential Storage Modality de la norme WebAuthn, ainsi que les définitions connexes des justificatifs détectables côté client et côté service [61]. Bien que l'U2F ne soit pas nécessairement considéré comme faisant partie de FIDO2, consultez également la section 7 de l'aperçu de l'authentification de second facteur (U2F) et la section 4.3 de la norme en matière de formats de messages

bruts U2F de FIDO Alliance (par exemple, « les jetons U2F peuvent encapsuler la clé privée générée et l'identifiant de l'application à laquelle la clé est destinée, et présenter le tout comme le pseudonyme de la clé »).

Bien qu'il soit admis que certains produits ne prennent en charge que des justificatifs détectables ou des solutions particulières, comme l'authentification sans mot de passe, les déclarations générales comme « la clé privée ne quitte jamais l'appareil » ne sont pas tout à fait exactes lorsqu'elles ont trait aux spécifications de FIDO Alliance et à la norme WebAuthn recommandée par le W3C. Il s'agit également d'une appellation erronée en ce qui concerne les clés d'accès synchronisées (voir ci-dessous pour en savoir plus).

Le principal avantage du stockage des clés privées sur le serveur est de diminuer la quantité de mémoire que doit posséder l'appareil, ce qui réduit le coût de l'authentifiant et permet théoriquement de prendre en charge un nombre illimité de paires de clés. Toutefois, la protection des clés privées stockées sur le serveur peut poser problème et dépend de la mise en œuvre adéquate d'un algorithme de chiffrement approuvé et des longueurs de clé connexes. Par exemple, Yubico utilise l'algorithme AES-256 en mode CCM (pour l'authentification de second facteur U2F, voir la page Web Key Generation). En outre, le nombre de clés d'accès pouvant être stockées sur les clés de sécurité FIDO2 ne cesse d'augmenter. Ainsi, une clé Yubikey 5 FIDO2 qui acceptait 25 clés d'accès liées à un appareil peut maintenant en accepter 100. De plus, Google a récemment lancé de nouvelles clés de sécurité Titan qui peuvent stocker plus de 250 clés d'accès (voir l'article intitulé The latest Titan Security Key is in the Google Store).

À noter également que la tendance actuelle de l'industrie semble s'orienter vers les clés d'accès qui sont, par définition, des justificatifs détectables et qui ne peuvent donc pas être stockées sur le serveur (voir le tableau B2

pour plus de contexte). Néanmoins, la modalité de stockage des justificatifs côté serveur ne doit pas être complètement écartée, puisqu'il existe des produits qui la mettent en œuvre.

B-3.3 Récupération

Comme avec toute autre méthode d'authentification, il doit y avoir un moyen de récupérer les authentifiants conformes à la norme FIDO lorsque l'authentifiant principal est égaré, volé ou endommagé. Selon FIDO Alliance (voir le document en ligne intitulé Recommended Account Recovery Practices for FIDO Relying Parties), il est recommandé que chaque utilisateur dispose d'au moins deux authentifiants conformes à la spécification FIDO, dont un authentifiant de secours au cas où il arriverait quelque chose à l'authentifiant principal. Toutefois, cette approche ne convient pas nécessairement au gouvernement du Canada, puisqu'elle entraîne une augmentation des coûts (en raison de la nécessité pour chaque utilisateur d'avoir plusieurs authentifiants), crée une expérience utilisateur négative et oblige les utilisateurs à stocker en toute sécurité leur(s) authentifiant(s) de secours. Par conséquent, d'autres méthodes de récupération doivent être explorées (par exemple, la mise en œuvre d'une approche d'authentification centralisée qui permettrait de prendre en charge d'autres approches appropriées). Les clés d'accès synchronisées (dont il a été question plus haut) ou les processus hybrides d'assurance élevée peuvent également constituer des solutions de rechange.

B-3.4 Attestation d'entreprise

Au départ, les spécifications de FIDO Alliance ont été conçues pour un marché de consommation de masse, à savoir les utilisateurs accédant à des services dans l'Internet. Bien que cela reste un objectif majeur, des ajouts récents à la norme WebAuthn recommandée et à la spécification CTAP introduisent la notion d'« attestation d'entreprise (AE) » afin de rendre les

authentifiants FIDO plus adaptés au domaine de l'entreprise. Cependant, la manière dont l'AE fonctionne réellement dans la pratique nécessite une étude plus approfondie.

À l'heure où nous écrivons ces lignes, les clés synchronisées ne permettent pas l'attestation [62]. En effet, la spécification CTAP 2.1 actuelle et la norme WebAuthn de niveau 2 recommandée ne prennent en charge l'attestation que pendant la procédure d'enregistrement. Il n'existe donc aucun moyen de faire valoir une nouvelle déclaration d'attestation au moment de l'authentification à partir d'un autre appareil avec une clé d'accès synchronisée. Toutefois, la prise en charge de cette nouvelle capacité devrait être ajoutée à la spécification CTAP 2.2 et à la norme WebAuthn de niveau 3 recommandée. Il reste à voir ce que cela signifiera dans la pratique et quel sera le niveau de soutien fourni par la communauté des fournisseurs.

Notez également que l'AE a été introduite dans le cadre de FIDO2 et qu'elle n'est pas prise en charge par l'authentification U2F.

Voir les pages Web FIDO TechNotes: The Truth About Attestation et FIDO Attestation White Paper pour en savoir plus sur l'attestation. La page Web Enterprise Attestation apporte des précisions sur l'AE, et plusieurs livres blancs relatifs aux déploiements d'entreprise sont disponibles dans le document en ligne intitulé Learn how FIDO authentication fits into your enterprise environment.

B-4 Termes clés

Les termes clés utilisés dans le présent document sont définis ci-dessous dans le tableau B1. Les définitions sont copiées ou extraites des sources indiquées dans la troisième colonne. Des précisions ont été ajoutées entre crochets à certaines définitions.

Tableau B1. Termes clés

Terme	Définition	Source
Authentifiant	Quelque chose que le demandeur [l'utilisateur] possède et contrôle (généralement un module cryptographique ou un mot de passe) et qui sert à authentifier l'identité du demandeur [l'utilisateur].	NIST SP 800-63-3
Authentifiant de plateforme	Authentifiant physiquement lié à un dispositif WebAuthn client donné, comme le module de plateforme sécurisée (TPM) d'un ordinateur portatif. La communication entre l'authentifiant et le dispositif WebAuthn client passe habituellement par une API propre à la plateforme. Authentifiant FIDO intégré à l'appareil de l'utilisateur.	Extrait de WebAuthn et d'autres sources Voir la page Web Platform Authenticator

Authentifiant itinérant	Authentifiant FIDO compatible avec n’importe quel dispositif à partir duquel l’utilisateur essaie de se connecter. Les authentifiants itinérants se connectent aux dispositifs des utilisateurs au moyen d’un protocole de transport comme USB, NFC ou Bluetooth. On les désigne souvent par le terme « clés de sécurité ». Un téléphone intelligent peut également servir d’authentifiant itinérant à l’aide de l’authentification inter-appareils FIDO. Authentifiant qui n’est pas physiquement lié à un dispositif WebAuthn client en particulier, comme la clé de sécurité ou les clés d’accès FIDO2 d’un téléphone mobile. Un authentifiant itinérant peut servir à s’authentifier auprès de plusieurs plateformes au moyen de différents protocoles de transport comme USB, BLE et NFC. Les authentifiants itinérants sont parfois appelés authentifiants multiplateformes ou externes.	Voir la page Web Roaming authenticator Extrait de la page Web WebAuthn et d’autres sources

Authentification inter-appareils (AIA)	L’authentification inter-appareils (AIA) de FIDO permet d’utiliser la clé d’accès d’un appareil pour se connecter à un service sur un autre appareil. Par exemple, votre téléphone peut être relié à votre ordinateur portatif, ce qui vous permet d’utiliser une clé d’accès de votre téléphone pour vous connecter à un service sur votre ordinateur portatif. L’AIA fait appel au protocole client-authentifiant (CTAP) de FIDO au moyen d’un transport « hybride ». Le protocole CTAP est mis en œuvre par les authentifiants et les plateformes clientes, et non par les parties de confiance. [Le transport hybride a été ajouté à la spécification CTAP 2.2 (voir la section 11.5), qui est actuellement au stade d’ébauche chez FIDO Alliance.]	Voir la section Cross-Device Authentication (CDA)

Clé d’accès (Voir également les entrées « Clé d’accès synchronisée » et « Clé d’accès liée à un appareil »)	Terme général, centré sur l’utilisateur final, qui désigne un justificatif FIDO2 ou WebAuthn détectable. À l’instar du terme « mot de passe », le terme courant « clé d’accès » s’emploie dans les conversations et les expériences de tous les jours. Orthographes en usage : « une clé d’accès » ou « des clés d’accès ». Les clés d’accès sont conçues pour simplifier la procédure de connexion. Toutes les clés d’accès peuvent offrir une expérience d’ouverture de session moderne, par exemple, avec une interface utilisateur à remplissage automatique ou un bouton « Se connecter avec une clé d’accès ». D’un point de vue technique, il existe deux types de clés d’accès : synchronisées et liées à un appareil. À noter que le terme clé d’accès est synonyme de justificatif détectable.	Voir la page Web Passkey
Clé d’accès liée à un appareil	Justificatif FIDO2 détectable lié à un seul authentifiant. Par exemple, les clés de sécurité FIDO2 contiennent généralement des clés d’accès liées à un appareil, puisque le justificatif ne peut pas quitter ce dernier. Les clés d’accès liées à un appareil étaient anciennement appelées **clés d’accès mono-appareils**. [Les clés d’accès liés à un appareil sont des justificatifs FIDO qui ne quittent jamais l’appareil et qui ne peuvent donc pas être synchronisés ou copiés.]	Voir la page Web Device-bound passkey

Clé d’accès synchronisée	Justificatif FIDO2 détectable et fiable permettant de se connecter sans autre forme d’authentification, comme un mot de passe à usage multiple ou unique. Par fiable, on entend que l’utilisateur peut se servir de la clé d’accès où et quand il en a besoin pour se connecter. Une telle disponibilité s’obtient par différents moyens. Par exemple, les fournisseurs de clés d’accès peuvent synchroniser celles-ci en temps réel entre les appareils d’un utilisateur, les restaurer à partir d’une sauvegarde chaque fois qu’un utilisateur configure un nouvel appareil, les offrir dans différents contextes (une clé établie à partir d’une application peut servir dans le navigateur lorsque l’utilisateur visite le site Web de l’application) ou permettre à l’utilisateur d’appliquer la clé d’accès entre différents appareils en utilisant par exemple la clé d’un téléphone à proximité pour se connecter à partir d’un ordinateur portatif. [Les clés d’accès synchronisés sont des justificatifs FIDO sauvegardés et accessibles sur plus d’un appareil.]	Voir la page Web Synced passkey

Interception (attaque de l'intercepteur)	Attaque par laquelle l'attaquant [l'auteur de la menace] s'immisce entre deux parties communicantes afin d'intercepter ou de modifier les données qui circulent entre elles. Dans le contexte de l'authentification, l'attaquant [l'auteur de la menace] s'immisce entre le demandeur [l'utilisateur] et le vérificateur, entre l'inscrit [l'utilisateur] et le fournisseur de justificatifs d'identité (FJI) au moment de l'inscription, ou entre l'abonné [l'utilisateur] et le FJI au moment de la liaison de l'authentifiant. [Anciennement appelé « attaquant du milieu » et également appelé « attaque de l'intercepteur ».]	NIST SP 800-63-3
Justificatif détectable	Un justificatif détectable (anciennement « justificatif résident » ou « clé résidente ») est un justificatif FIDO2 ou WebAuthn entièrement stocké dans l'authentifiant (clé privée, code du justificatif, pseudonyme de l'utilisateur et autres métadonnées). La partie de confiance conserve également une copie de la clé **publique** et du code du justificatif. Également connu sous le nom de justificatif détectable côté client, un justificatif détectable a une modalité de stockage côté client et peut être détecté [ou récupéré] sans que l'utilisateur ait à fournir à la partie de confiance des renseignements préalables à l'authentification.	Voir la page Web Discoverable Credential Extrait de la page Web WebAuthn

Justificatif multidispositifs (Voir également l'entrée « Clé d'accès synchronisée »)	Justificatif FIDO qui peut être sauvegardé et copié dans plusieurs appareils. Également appelé « clé d'accès synchronisée ». Exemples : • Connexion sans mot de passe avec des clés d'accès • Utiliser des clés d'accès pour se connecter à des sites web et des apps sur l'iPhone	Extrait du document FIDO Deploying Passkeys in the Enterprise: Introduction
Justificatif non détectable	Également connu sous le nom de justificatif côté serveur, un justificatif non détectable a une modalité de stockage côté serveur et ne peut pas être « détecté » (ou récupéré) sans que l'utilisateur fournisse des renseignements à la partie de confiance.	Extrait de la page Web WebAuthn
Modalité de stockage des justificatifs	Déterminée par l'endroit où la clé privée du justificatif est stockée, soit du côté client (justificatif détectable) soit du côté serveur (justificatif non détectable). Dans le cas d'une modalité de stockage du justificatif côté serveur, la clé privée du justificatif est chiffrée (encapsulée) à l'aide d'un puissant algorithme de chiffrement symétrique (comme AES-256), de sorte que seul cet authentifiant peut la déchiffrer (c.-à-d. la désencapsuler). La clé privée du justificatif est stockée par la partie de confiance (paramètre Code du justificatif dans la source du justificatif de la clé publique) et retournée à l'authentifiant au moyen de l'option allowCredentials de la commande get(), ce qui permet à l'authentifiant de déchiffrer et d'utiliser la clé privée du justificatif.	Extrait de la page Web WebAuthn, Section 6.2.2: Credential Storage Modality

Protocole client-authentifiant (CTAP)	Protocole de couche d'application servant à la communication entre un authentifiant itinérant et un autre client ou une autre plateforme, ainsi que les liaisons de ce protocole d'application à un éventail de protocoles de transport utilisant différents supports matériels.	Spécification CTAP 2.1
Résistance à l'hameçonnage	Capacité du protocole d'authentification de détecter les secrets d'authentification et les résultats valides de l'authentifiant et d'empêcher leur divulgation à une fausse partie de confiance, indépendamment du niveau de vigilance de l'abonné [l'utilisateur].	NIST SP 800-63B-4 (section 5.2.5)

Le tableau B2 présente une synthèse des relations entre les différents termes ou concepts associés aux justificatifs FIDO pour en faciliter la mise en contexte.

Tableau B2. Relations entre les termes associés aux justificatifs FIDO

	Justificatif détectable?	**Constitue une clé d'accès?**	**Peut se synchroniser?**
Justificatif multidispositifs	Oui	Oui (« clé d'accès synchronisable »)	Oui
Justificatif lié à un appareil	Oui	Oui (« clé d'accès liée à un appareil »)	Non
Justificatif côté serveur	Non (non détectable)	Non [63]	Non

Note de mise en œuvre (sous réserve de modifications) : Selon Yubico, Android est « le seul système d'exploitation mobile grand public capable de générer des justificatifs liés à un seul appareil ». Il en va tout autrement avec Apple iOS, qui stocke les clés d'accès dans un trousseau iCloud et les

synchronise entre les appareils enregistrés de l'utilisateur. De plus, ce système d'exploitation comporte le service AirDrop, qui permet de partager des clés d'accès avec d'autres personnes. Pour en savoir plus :

- À propos de la sécurité des clés d'identification
- Utiliser des clés d'accès pour se connecter à des applications et des sites web sur l'iPhone
- Partager en toute sécurité des clés d'accès et des mots de passe avec AirDrop sur l'iPad

Annexe C : Vue d'ensemble et comparaison des modules de plateforme sécurisée

La dernière version de la spécification de module de plateforme sécurisée (TPM), publiée par le Trusted Computing Group, est TPM 2.0. Cette version apporte diverses améliorations à la version 1.2 qui la précède. Le document Trusted Platform Module (TPM) 2.0: A Brief Introduction présente une vue d'ensemble de la spécification TPM 2.0 et résume les cinq différents types de modules comme suit :

- **TPM discret.** Fournit le niveau de sécurité le plus élevé qui permet, par exemple, de protéger la commande de frein d'une voiture. Il élimine tout risque de piratage de l'appareil qu'il protège, quelle que soit la complexité des méthodes malveillantes employées. À cette fin, la puce discrète est conçue, fabriquée et évaluée au niveau de sécurité le plus élevé contre la falsification, notamment le sondage et le gel perpétrés par toutes sortes d'attaques avancées.
- **TPM intégré.** Arrive en deuxième en termes de sécurité. Il s'agit ici encore d'un composant matériel, mais intégré cette fois à une puce

dont les fonctions ne sont pas axées sur la sécurité. Son implémentation matérielle le rend résistant aux bogues logiciels, mais pas aux falsifications matérielles.

- **TPM microprogramme.** Est mis en œuvre dans les logiciels protégés. Une puce distincte n'est pas nécessaire, puisque c'est le processeur principal qui exécute le code du module. Bien qu'il s'exécute comme n'importe quel autre programme, le code se trouve dans un environnement d'exécution protégé, appelé « environnement d'exécution de confiance » (EEC), qui est isolé du reste des programmes que le processeur exécute. Ainsi, les secrets dont le TPM peut avoir besoin, mais auxquels les autres programmes ne doivent pas avoir accès, comme les clés privées, peuvent être conservés dans l'EEC, ce qui rend la tâche plus difficile aux pirates informatiques. L'inconvénient du TPM microprogramme, outre sa vulnérabilité aux falsifications, est que sa sécurité dépend de nombreux autres facteurs, notamment le système d'exploitation de l'EEC, les bogues dans le code de l'application exécutée dans cet environnement, et bien d'autres encore.
- **TPM logiciel.** Peut être mis en œuvre comme un émulateur logiciel du TPM. Il est cependant exposé à de nombreuses vulnérabilités, non seulement à la falsification, mais aussi aux bogues de tout système d'exploitation qui l'utilise. Parmi ses principales applications, mentionnons qu'il s'avère très utile pour concevoir ou mettre à l'essai un prototype de système auquel un TPM est intégré. Dans le cadre de tels essais, un TPM logiciel pourrait constituer la bonne solution et la bonne approche.
- **TPM virtuel.** De nombreux systèmes d'Internet des objets (IdO) comprennent des capteurs et des processus de traitement en nuage, ce qui nécessite des capacités de virtualisation. Dans un

environnement infonuagique, un moyen astucieux de mettre en œuvre un TPM est de le virtualiser. Le TPM virtuel fait partie de l'environnement infonuagique et offre les mêmes commandes que son équivalent matériel, mais il les fournit séparément à chaque machine virtuelle.

Le tableau C1 compare les différents types de TPM. Il s'agit d'une reproduction partielle du tableau présenté dans le document Trusted Platform Module (TPM) 2.0: A Brief Introduction, auquel on a ajouté les colonnes « Type d'authentifiant » et « LoA » (niveau d'assurance). Il convient de noter que le niveau d'assurance le plus élevé possible suppose que **toutes** les exigences de ce niveau sont satisfaites, y compris les niveaux appropriés de la certification FIPS 140-3 et les autres facteurs applicables. À noter que l'ajout de ces colonnes découle d'une évaluation globale préliminaire qu'il faudra approfondir, en particulier en ce qui a trait aux niveaux d'assurance des TPM microprogrammes et virtuels.

Tableau C1. Comparaison des TPM

Type de TPM	Sécurité relative	Environnement d'exécution	Type d'authentifiant	LoA le plus élevé possible
TPM discret	La plus élevée	Puce matérielle dédiée et inviolable	Dispositif cryptographique multifactoriel ou à un facteur	LoA 4
TPM intégré	Supérieure	Composant matériel distinct, non dédié aux fonctions de sécurité et non inviolable	Dispositif cryptographique multifactoriel ou à un facteur	LoA 3

Type de TPM	Sécurité relative	Environnement d’exécution	Type d’authentifiant	LoA le plus élevé possible
TPM microprogramme	Élevée	EEC dans le processeur	Logiciel cryptographique multifactoriel ou à un facteur	LoA 3
TPM logiciel	Aucune	Système d’exploitation	Logiciel cryptographique multifactoriel ou à un facteur	LoA 1
TPM virtuel	Élevée	Hyperviseur	Logiciel cryptographique multifactoriel ou à un facteur	LoA 3

À noter qu’au niveau d’assurance 4, il faut utiliser un TPM discret pour générer et stocker en toute sécurité la ou les clés de signature privées et effectuer les opérations cryptographiques du processus d’authentification de l’utilisateur (p. ex., la clé privée sert à signer numériquement un nonce – un nombre arbitraire à usage unique – dans un protocole d’authentification de simulation-réponse). En outre, les clés privées ne doivent pas être exportables. Autrement dit, elles ne doivent jamais quitter le TPM discret. Il faut également savoir que les TPM logiciels se limitent aux étapes des essais et du prototypage et ne doivent jamais servir par la suite.

Notes de bas de page

1 Source : CBC News | Spy agency chief says new powers would help stop cyberattacks before they happen [en anglais seulement].

2 Source : CBC News | Spy agency chief says new powers would help stop cyberattacks before they happen [en anglais seulement]. Cette référence date de 2018, mais elle illustre bien le fait que les systèmes et les données du GC sont des cibles lucratives. Il est également raisonnable de penser que le nombre d'interventions malveillantes n'a fait qu'augmenter.

3 Le NIST a publié la deuxième version publique des *Digital Identity Guidelines*, y compris la NIST SP 800-63B-4 (deuxième version publique) [en anglais seulement] après que le présent document a été soumis au processus de publication officiel. Bien qu'il y ait des changements importants par rapport à la première version publique, ces changements n'ont pas d'incidence considérable sur les recommandations formulées dans le présent document. Certains de ces changements sont mentionnés dans le présent document.

4 Ce concept est souvent représenté par « l'identifiant et le mot de passe ». Cependant, l'identifiant n'est pas nécessairement, et typiquement, connu seulement de l'utilisateur. C'est toujours la combinaison de l'identifiant et du mot de passe qui est considérée comme une A1F, puisque les deux éléments doivent être utilisés ensemble.

5 Les authentifiants à renseignement préenregistré (p. ex., les réponses préétablies à une série de questions difficiles) ne sont plus considérés comme acceptables et ne sont donc pas inclus dans les exemples de quelque chose que vous connaissez. Ils ont été supprimés de la NIST SP 800-63B et devraient également l'être dans la prochaine mise à jour de l'ITSP.30.031.

6 Certains produits MPU 1F demandent à l'utilisateur d'appuyer sur un bouton pour afficher le code à usage unique, mais le fait d'appuyer sur le bouton ne constitue pas un deuxième facteur d'authentification. Il existe également des produits MPU 1F qui ne nécessitent pas que l'utilisateur appuie sur un bouton (l'écran est toujours allumé, et les codes changent automatiquement après un certain laps de temps).

7 Notez que les données biométriques peuvent seulement être utilisées pour l'authentification locale, et non pour l'authentification à distance. Par exemple, l'empreinte digitale d'un utilisateur peut être utilisée pour déverrouiller ou activer un authentifiant matériel de chiffrement MF. Voir la section 5.2.3 de la NIST SP 800-63B pour une liste de restrictions et des renseignements supplémentaires.

8 Cette définition vient de la section 5.2.3 de la NIST SP 800-63B.

9 Notez que la section 5.1.4 de la NIST SP 800-63B inclut à la fois les dispositifs matériels et les générateurs MPU logiciels installés sur des appareils mobiles dans cette catégorie. L'ITSP.30.031 v3 ne traite pas explicitement des applications MPU logicielles.

10 La section 5.1.6 de la NIST SP 800-63B présente un nouvel authentifiant cryptographique logiciel 1F, lequel devrait également être ajouté à la prochaine version de l'ITSP.30.031.

11 La version 4 des *Digital Identity Guidelines* du NIST introduit un nouvel authentifiant HB MF. Le NIST le définit comme un dispositif physique indépendamment adressable et qui peut communiquer en toute sécurité avec le vérificateur sur un canal de communication distinct appelé canal secondaire.

12 La section 4.3.1 de l'ITSP.30.031 v3 indique qu'un authentifiant cryptographique logiciel MF est de niveau AAL1/LoA 2; cette décision était cependant fondée sur les déficiences liées à l'authentifiant logiciel maCLÉ. Même si ces lacunes subsistent et qu'un authentifiant logiciel maCLÉ reste au LoA 2, il existe des exemples d'authentifiants logiciels MF qui pourraient être considérés au LoA 3. On s'attend donc à ce que la prochaine mise à jour de l'ITSP.30.031 rétablisse ce type d'authentifiant (mais pas un authentifiant logiciel maCLÉ) au LoA 3 en tant que LoA le plus élevé **possible**.

13 La section 5.1.5 de la NIST SP 800-63B inclut à la fois les dispositifs matériels et les générateurs MPU logiciels installés sur des dispositifs mobiles dans la catégorie « OTP device » (dispositifs MPU). Cela a été clarifié dans la NIST SP 800-63B-4 (deuxième version publique). L'ITSP.30.031 v3 ne traite pas explicitement des applications MPU logicielles.

14 Les *Digital Identity Guidelines* du NIST ne considèrent plus qu'un authentifiant matériel MPU MF, en soi, est suffisant pour atteindre le niveau AAL3/LoA 4 (puisqu'il n'est pas résistant à l'hameçonnage).

15 La version 3 des *Digital Identity Guidelines* du NIST définissait plusieurs autres combinaisons d'authentifiants au niveau AAL3/LoA 4 qui sont omises ici puisqu'elles ne sont plus incluses dans la NIST SP 800-63B-4 (deuxième version publique) et n'ont jamais été incluses à titre d'exemples dans les figures 2.1 et 2.2 du présent document.

16 Une attaque par notification poussée ou demande d'AMF répétée ou un bombardement de notifications poussées consiste à bombarder un utilisateur de notifications poussées d'applications mobiles jusqu'à ce qu'il approuve une demande par accident ou par agacement. Les notifications poussées avec numéro à saisir permettent de s'assurer que l'utilisateur essaie réellement de s'authentifier. Voir le document Implementing Number Matching in MFA Applications [en anglais seulement] de la Cybersecurity and Infrastructure Security Agency des États-Unis pour de plus amples renseignements.

17 De plus, bien qu'un téléphone intelligent et un authentifiant matériel MPU puissent tous deux être volés, il est plus facile de protéger un authentifiant matériel MPU contre le vol. On peut, par exemple, attacher l'authentifiant au même cordon que la carte d'accès de l'utilisateur, ce qui le rend plus difficile à voler. On peut également faire valoir qu'un téléphone intelligent est généralement une cible plus attrayante, puisqu'il a une valeur qui dépasse le contexte de l'authentification, ce qui n'est pas le cas d'un authentifiant matériel MPU.

18 L'exigence pour un authentifiant distinct indépendant de la plateforme est basée sur les conseils fournis par le CCC.

19 Source : Section 5.2.5 de la NIST SP 800-63B-4 (Revision 4, Initial Public Draft) [en anglais seulement].

20 La méthode utilisée pour attirer l'utilisateur sur le faux site Web n'a pas d'importance dans le contexte.

21 Cela ne signifie pas qu'il n'est pas nécessaire de prendre des mesures de sécurité supplémentaires si l'un des authentifiants est intrinsèquement résistant à l'hameçonnage. Voir la section 2.4.6.

22 Pour ce faire, il est possible d'utiliser des certificats d'appareils (de préférence avec les clés privées associées conservées en toute sécurité dans du matériel validé FIPS 140).

23 Ce mémorandum adopte les authentifiants FIDO résistants à l'hameçonnage comme solution de rechange aux cartes de vérification de l'identité personnelle (VIP).

24 Le document Trusted Platform Module (TPM) 2.0 : A Brief Introduction [en anglais seulement] présente une vue d'ensemble de la spécification TPM 2.0 et résume les cinq différents types de modules. Voir également l'annexe C du présent document.

25 Introduction to Secure Elements [en anglais seulement] présente une introduction générale aux ES.

26 Introduction to Trusted Execution Environments [en anglais seulement] présente un aperçu général des EEC.

27 Source : Tiré des sections 5.1.6.1 et 5.1.8.1 de la NIST SP 800-63B.

28 Il ne s'agit pas d'exclure la possibilité d'utiliser la modalité de stockage des justificatifs d'identité côté serveur au niveau AAL2/LoA 3 (voir la section 2.3.7.1). La prise en charge des clés d'accès synchronisées à ce niveau pourrait être possible ultérieurement (voir la section 2.3.7.2).

29 L'utilisateur doit utiliser correctement les authentifiants indépendants de la plateforme afin de pouvoir bénéficier des avantages supplémentaires qu'ils offrent en matière de sécurité par rapport aux authentifiants liés à une plateforme. Il s'agit notamment de maintenir le contrôle positif de l'authentifiant par l'utilisateur à tout moment et, s'il est physiquement connecté pendant l'utilisation, de retirer l'authentifiant de la plateforme informatique lorsqu'il n'est pas utilisé.

30 Source : les sections 5.1.8.1 et 5.1.9.1 de la NIST SP 800-63B-4 (version 4, première version publique).

31 Au moment de la rédaction du présent document, la version en vigueur de la norme FIPS 140 (*Security Requirements for Cryptographic Modules*) est la FIPS 140-3. Les modules cryptographiques validés par rapport à la version précédente, la norme FIPS 140-2, restent valables. Dans le présent document, les références à la FIPS 140 doivent être interprétées comme étant les versions FIPS 140-2 ou FIPS 140-3. Voir le Cryptographic Module Validation Program [en anglais seulement] pour de plus amples renseignements.

32 Anciennement appelé « attaquant du milieu » et également appelé « attaque de l'intercepteur ».

33 Source : Tiré de la définition dans la NIST SP 800-63-3.

34 Source : Tirée de la section 5.2.8 de la NIST SP 800-63B.

35 L'ITSP.30.031 v3 (voir la section 6.3) indique que la résistance à la réinsertion est obligatoire même au LoA 1 (ce qui découle de la directive *Electronic Authorization Guideline*, aujourd'hui obsolète, du NIST). Toutefois, la NIST SP 800-63B indique que la résistance à la réinsertion n'est pas obligatoire au AAL1/LoA 2. Pour l'instant, nous l'avons recommandé au LoA 2, mais l'information sera harmonisée ultérieurement avec l'ITSP.30.031v4.

36 Si les justificatifs côté serveur sont pris en charge, les clés privées doivent être chiffrées à l'aide d'un puissant algorithme de chiffrement symétrique, comme le recommande l'ITSP.40.111, et le module cryptographique doit être validé FIPS 140, comme l'indique la section 2.3.3.

37 Comme indiqué dans la section 2.3.7.2, il est possible d'apporter des modifications afin d'inclure l'attestation pendant l'authentification.

38 Source : Client to Authenticator Protocol (CTAP), 2.1, Section 7.1 [en anglais seulement].

39 Cela pourrait également être utilisé pour remplacer l'ID utilisateur et le mot de passe par un authentifiant sans mot de passe 1F résistant à l'hameçonnage.

40 Des limites de temporisation plus courtes peuvent être requises dans certains cas.

41 Inviter l'utilisateur à effectuer une action avant que le délai d'inactivité ne soit écoulé peut éviter une réauthentification inutile et donc entraîner moins de frictions pour celui-ci. Il peut s'agir d'une simple question du type « Êtes-vous toujours là? » Veuillez noter que la réponse ne réinitialise que le délai d'inactivité de l'utilisateur, et non la durée de la session, puisqu'il n'y a pas eu de réauthentification.

42 *Ibid*.

43 Source : Tiré de la définition du NIST dans Risk Adaptive (Adaptable) Access Control [en anglais seulement].

44 Gartner décrit un modèle similaire appelé « Continuous Adaptive Risk and Trust Assessment » (CARTA); voir le document *Zero Trust is an Initial Step on the Roadmap to CARTA* de Gartner [en anglais seulement].

45 Au moment d'écrire ces lignes, on s'attend à ce qu'il s'agisse de clés d'accès liées à un appareil; les clés d'accès synchronisées pourraient cependant être autorisées ultérieurement. Voir les sections 2.3.7.2 et 2.3.7.3 pour de plus amples renseignements.

46 Les expressions « mot de passe robuste » et « mot de passe robuste et bien géré » utilisées dans le présent document font référence à des pratiques de composition et de gestion des mots de passe qui répondent aux exigences de l'*Orientation sur les mots de passe* du GC.

47 Voir les *Mesures de protection du nuage du gouvernement du Canada* et les références connexes pour plus de renseignements.

48 Il convient de noter que la version originale du document OMB M-04-04 des États-Unis (désormais annulé) traitait de « potential impact » (répercussions potentielles) et que cette notion est maintenant abordée brièvement dans la section 5.3 du document SP 800-63-3 du NIST. Cependant, en ce qui concerne les authentifiants, il est en fait question du niveau de confiance selon lequel ceux-ci sont correctement liés à l'utilisateur et sous le contrôle de ce dernier, ainsi que du niveau de confiance selon lequel les authentifiants ont été compromis ou non.

49 Dans le document ITSP.30.031v3, on utilise le terme « jeton » plutôt que « authentifiant », ce qui est conforme au document SP 800-63-3 du NIST, aujourd'hui remplacé. Dans le nouveau document *Digital Identity Guidelines* du NIST, le terme « tokens » (jetons) est remplacé par « authenticators » (authentifiants). On s'attend à ce que la prochaine mise à jour du document ITSP.30.031 intègre cette modification terminologique.

50 Cependant, la *Ligne directrice sur la définition des exigences en matière d'authentification* reconnaît que le LoA cible peut ne pas toujours être atteignable en pratique et prévoit donc des mesures compensatoires et une gestion des risques lorsque cela est nécessaire.

51 De plus, le document OMB M-04-04 a été annulé en mai 2019 après la publication du document OMB M-19-17, qui marque officiellement l'abandon par le gouvernement fédéral des États-Unis du modèle à quatre niveaux d'assurance.

52 Il convient de noter que la version 4 des *Digital Identity Guidelines* du NIST est en cours d'élaboration et qu'elle devrait au minimum entraîner la modification de certaines de ces définitions et de ces mises en correspondance.

53 Dans la version 3, ce niveau semble comprendre les deux niveaux. Cependant, dans la version 4 provisoire des *Digital Identity Guidelines* du NIST, l'IAL1 devient l'IAL0 (aucune confirmation de l'identité) et l'IAL2 est scindé en deux, IAL1 et IAL2; il pourrait donc être plus simple de lier les IAL aux LoA du GC. Ce point est à revoir une fois que la version 4 sera achevée et officiellement publiée en remplacement de la version 3. Les correspondances **pourraient** être les suivantes : l'IAL0 correspond au LoA de l'identité 1, l'IAL1 correspond au LoA de l'identité 2, l'IAL2 correspond au LoA de l'identité 3, et l'IAL3 correspond au LoA de l'identité 4.

54 La version 3 et la version 4 provisoire semblent présenter de grandes différences en ce qui concerne les FAL. Ce point est à revoir une fois que la version 4 sera officiellement publiée en remplacement de la version 3.

55 Selon le document SP 800-63C du NIST, ce niveau est équivalent au profil client de base d'OpenID Connect (c'est-à-dire le flux de code d'autorisation du canal d'appui) et au profil SAML Web Browser Single-Sign-On, qui utilise des liaisons d'artéfacts du canal d'appui.

56 Le document SP 800-63C du NIST indique que le FAL2 ou un niveau supérieur est requis pour le canal d'avant-plan (c'est-à-dire la liaison de redirection SAML ou le flux implicite OpenID Connect).

57 Dans le profil SAML 2.0 Web Browser Single-Sign-On, on appelle ce type d'assertion « holder-of-key » (détenteur de la clé).

58 Citation de plusieurs sources sur FIDO Alliance.

59 Source : Extrait de la spécification Client to Authenticator Protocol (CTAP) [en anglais seulement] et du site Web de FIDO Alliance [en anglais seulement].

60 Source : Section 1.1 de la spécification CTAP [en anglais seulement].

61 Source : Site Web de FIDO Alliance [en anglais seulement].

62 Les clés privées stockées sur l'appareil étaient auparavant appelées « clés résidentes » ou « justificatifs résidents », mais sont dorénavant appelées « justificatifs détectables côté client » ou simplement « justificatifs détectables ». Les clés privées stockées (sous forme chiffrée) sur le serveur étaient appelées « clés non résidentes », mais sont dorénavant appelées « justificatifs côté serveur » ou « justificatifs non détectables ».

63 Par exemple, le livre blanc de FIDO Alliance, intitulé FIDO Authentication for Moderate Assurance Use Cases [en anglais seulement] et daté de juin 2023, précise qu'« au moment de la publication, les clés d'accès synchronisées ne mettent pas en œuvre l'attestation, ce qui signifie qu'elles ne constituent pas une solution adaptée aux utilisateurs qui détiennent des privilèges élevés et qui nécessitent des niveaux d'assurance plus élevés ou aux organisations qui souhaitent mettre en œuvre l'AE ». [traduction]

64 Voir les pages Web Discoverable vs non-discoverable credentials [en anglais seulement] et Discoverable Credential [en anglais seulement] pour des exemples.

ISBN : 978-0-660-76818-2

Date de modification : 2025-05-23

xx
yy