SANTÉ QUÉBEC

Orientation sur l’authentification à facteurs multiples (MFA)

Date : 2025-12-19

Objectif

Définir des mesures de sécurité rigoureuses lors de l'intégration des sources d'identité afin de protéger les données sensibles des Dossiers Médicaux Électroniques (DMÉ) et des Systèmes d'Information de Pharmacie Communautaire (SIPC).

Bonnes pratiques

Dans le cadre de la certification des produits et services technologiques du secteur de la santé et des services sociaux, le Bureau de certification recommande fortement :

- de toujours privilégier les sources officielles : Azure AD provincial, SFiD ou autres identités reconnues par le MSSS, lorsque possible.
- d'appliquer strictement les directives ci-dessous.

Titre :	**Exigences liées à l'authentification à facteurs multiples**
Mots clés :	GIA; multifacteur; authentification forte; facteurs multiples; multifactoriel; MFA; 2FA; AMF
Raison :	Les mots de passe peuvent facilement être exposés et compromis. L'authentification à facteurs multiples ou authentification forte renforce la sécurité offerte par ces mots de passe en exigeant différentes formes de vérification permettant de valider l'identité **hors de tout doute raisonnable** lors de la connexion à un actif informationnel ou un service.

Tout actif doit utiliser une authentification à facteurs multiples pour un niveau d'assurance raisonnable de l'authentification AU2, AU3 ou AU4

Clarification :
Un choix de facteurs d'authentification doit être offert par le fournisseur d'identité[1], à tout utilisateur qui doit accéder à un actif informationnel ou à un service, dans le respect du niveau d'authentification requis pour y accéder.

Les systèmes d'authentification ont recours à trois types de facteurs dont les caractéristiques générales sont:

#	Caractéristique	Description	Exemple
1	Élément connu de l'utilisateur « Quelque chose que vous savez »	Information que seul l'utilisateur légitime devrait savoir	• Mot de passe • NIP
2	Élément que l'utilisateur possède « Quelque chose que vous avez »	Élément matériel que seul l'utilisateur légitime possède et contrôle	• Appareil mobile • Clé physique • Jeton matériel
3	Élément que l'utilisateur produit ou qui le caractérise « Quelque chose que vous êtes »	Attribut physique unique à chaque utilisateur	• Empreinte digitale • Voix

Raison :	• Mettre en place un niveau d'authentification en adéquation avec le niveau de sensibilité des actifs informationnels. • Augmenter le niveau de sécurité des actifs par une authentification à facteurs multiples • Appliquer l'exigence 4 des 15 mesures de sécurité minimales du MCN • Appliquer les exigences 1, 2, 3 et 4 des 12 exigences de sécurité minimales dans l'infonuagique
Info :	15 mesures de sécurité minimales – MCN 12 exigences minimales pour l'infonuagique - MCN Cadre de confiance pancanadien (CCP) du Conseil canadien de l'identification et de l'authentification numériques (CCIAN)

---

[1] Un fournisseur d'identité (abrégé IdP ou IDP) est une entité ou un système qui crée, maintient et gère les informations d'identité pour les mandants et fournit également des services d'authentification aux applications clientes au sein d'une fédération ou d'un réseau distribué. (Wikipédia)

Le fournisseur d'identité doit offrir deux types de facteurs différents pour assurer l'authentification à facteurs multiples.		
Clarifications : L'authentification à facteurs multiples nécessite l'utilisation de deux types de facteurs d'authentification que le fournisseur d'identité met à la disposition d'un utilisateur selon son niveau d'authentification. Ces facteurs doivent être indépendants, comme le montrent les trois exemples de combinaisons suivants :		
D'un secret mémorisé (mot de passe : quelque chose que vous savez)	**Et**	D'un dispositif hors bande (un canal secondaire différent du poste de travail : quelque chose que vous avez)
D'un secret mémorisé (mot de passe: quelque chose que vous savez)	**Et**	D'un mot de passe à usage unique (OTP (One Time Password)) (matériel ou logiciel : quelque chose que vous avez)
D'un secret mémorisé (mot de passe: quelque chose que vous savez)	**Et**	D'un dispositif d'identification physique (matériel ou logiciel : quelque chose que vous êtes)

Raison :	Le fournisseur d'identité doit fournir un choix de facteurs d'authentification à toute personne qui accède à un actif informationnel ou à un service incluant les cas particuliers.
Info :	• Règles relatives à l'assurance de l'identité numérique : Arrêté numéro 2022-05 du ministre de la Cybersécurité et du Numérique • Cadre de confiance pancanadien (CCP) du Conseil canadien de l'identification et de l'authentification numériques (CCIAN)

Une authentification à facteurs multiples de base est offerte pour le niveau d'assurance de l'authentification AU2
Clarification : L'AU1 est un niveau d'assurance de l'authentification où un seul facteur serait suffisant, par exemple l'utilisation d'un nom d'utilisateur et un mot de passe. (**Ce niveau n'est pas jugé adéquat pour passer le processus de certification**) Lorsqu'un niveau d'assurance de l'authentification AU2 (moyen) est requis, une combinaison de deux types de facteurs d'authentification différents doit être utilisée.
Par exemple, il serait acceptable d'utiliser en plus d'un nom d'utilisateur et un mot de passe, un des facteurs suivants : • un code à utilisation unique (facteur de type « quelque chose que vous avez »); • la transmission à la personne concernée par des modes qui peuvent inclure : o l'appel téléphonique (SMS ou appel vocal); o le courriel; o le courrier papier.

Raison :	L'actif est de niveau AU2, il est classifié moyen selon la grille d'analyse de préjudices sur les niveaux d'assurance d'authentification[2].
Info :	Voir les liens précédents.

---

[2] Une grille d'analyse de préjudices sur les niveaux d'assurance de l'authentification est mise en place afin de fournir une base uniforme sur laquelle s'appuyer lors de l'analyse des risques liés à la sécurité de l'actif.

Une authentification à facteurs multiples avancée est offerte pour le niveau d'assurance de l'authentification AU3 **Niveau minimal exigé pour tout PST traitant des renseignements de santé ou de services sociaux ou arrimé avec un actif informationnel d'intérêt commun traitant des renseignements de santé ou de services sociaux.**	
Clarification : Pour un niveau d'assurance de l'authentification AU3 (élevé), deux types de facteurs d'authentification différents doivent être utilisés. Le deuxième facteur doit être de sécurité supérieure à ceux utilisés dans AU2 afin de favoriser la réduction des risques[3] en fonction du niveau de sensibilité de l'information.	
Pour un facteur de type « quelque chose que vous avez », les deuxièmes facteurs les plus souvent utilisés sont : • le jeton cryptographique; • le certificat; • le jeton logiciel; • le code à usage unique; • l'application sollicitant une approbation; • toute autre méthode jugée équivalente; • … autres. Les modes de transmission d'un code à utilisation unique suivants **sont interdits**: • le SMS; • l'appel vocal; • la télécopie (fax); • le courriel; • le courrier papier.	
Raison :	Le niveau d'assurance AU3 exigence un niveau de sécurité supérieur.
Documentation :	Voir les liens précédents.

Une authentification à facteurs multiples avancée incluant un dispositif cryptographique est offerte pour le niveau d'assurance de l'authentification AU4
Clarification : ➔ Les exigences de ce niveau d'authentification seront précisées ultérieurement.

---

[3] Voir la section [*8.1 Menaces liées à l'authentification*] de la « Publication spéciale NIST 800-63B » (en anglais)