A.M., 2022

Arrêté numéro 2022-05 du ministre de la Cybersécurité et du Numérique en date du 26 août 2022

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement
(chapitre G-1.03)

CONCERNANT les Règles relatives à l'assurance de l'identité numérique

LE MINISTRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE,

VU le deuxième alinéa de l'article 21 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03) suivant lequel le ministre de la Cybersécurité et du Numérique peut déterminer des orientations portant sur les principes ou les pratiques à appliquer en matière de gestion des ressources informationnelles, incluant les pratiques pour optimiser l'organisation du travail de même que la nécessité de considérer l'ensemble des technologies offrant un potentiel d'économies ou de bénéfices et des modèles de développement ou d'acquisition disponibles pour répondre aux besoins des organismes publics, dont les logiciels libres;

VU le paragraphe 2° de l'article 12.6 de cette loi suivant lequel le chef gouvernemental de la sécurité de l'information assume la responsabilité de recommander au ministre de la Cybersécurité et du Numérique des règles pour assurer la sécurité de l'information, incluant celles relatives à l'authentification et à l'identification;

VU la recommandation du chef gouvernemental de la sécurité de l'information, en date du 28 juillet 2022, au ministre de la Cybersécurité et du Numérique au regard des Règles relatives à l'assurance de l'identité numérique, annexées au présent arrêté;

CONSIDÉRANT qu'il y a lieu, pour le ministre de la Cybersécurité et du Numérique, de déterminer des orientations concernant l'authentification et l'identification en matière de sécurité de l'information, soient celles déterminées dans les Règles relatives à l'assurance de l'identité numérique, annexées au présent arrêté;

ARRÊTE CE QUI SUIT :

DÉTERMINE des orientations concernant l'authentification et l'identification en matière de sécurité de l'information, soient celles déterminées dans les Règles relatives à l'assurance de l'identité numérique, annexées au présent arrêté.

Québec, le 26 août 2022

Le ministre de la Cybersécurité et du Numérique,
ÉRIC CAIRE

Règles relatives à l'assurance de l'identité numérique

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement
(chapitre G-1.03, a. 21)

SECTION I
DISPOSITIONS INTRODUCTIVES

1. Les présentes règles prévoient des dispositions relatives à l'assurance de l'identité numérique permettant d'assurer que la personne qui entend utiliser ou autrement bénéficier d'un service numérique d'un organisme public, étant un service faisant appel aux technologies de l'information, est bien celle qu'elle prétend être, notamment en prévoyant la détermination de niveaux d'assurance de l'identité.

Elles prévoient également les exigences à respecter lors de l'identification et de l'authentification d'une telle personne, tout en offrant un degré de confiance suffisant pour la prestation du service concerné.

Elles doivent être appliquées dans le respect de la Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1) et peuvent être complétées par toute indication d'application que peut formuler le chef gouvernemental de la sécurité de l'information en vertu du paragraphe 4° de l'article 12.6 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03).

2. Dans les présentes règles, on entend par :

1° « agent » : la fonction visée à l'article 17;

2° « assurance de l'identité numérique » : l'ensemble des activités liées à l'identification et à l'authentification visées aux sous-sections 2 et 3 de la section III;

3° « attribut de base » : au regard d'une personne physique, soit son nom, son prénom, sa date de naissance, son lieu de naissance ou les noms et prénoms de ses parents alors qu'au regard d'une entreprise ou d'une autre entité, soit son nom ou ses coordonnées;

4° « attribut de l'identité » : au regard d'une personne, outre un attribut de base, tout autre élément pouvant lui être associé ou pouvant être combiné pour permettre son identification de manière unique et sans équivoque;

5° « authentification multifacteur » : l'authentification de base ou avancée qui met en œuvre, de façon concomitante, au moins deux facteurs d'authentification distincts constituant une méthode d'authentification forte;

6° « justificatif » : un élément tangible ou logique unique émis à une personne ou en lien avec celle-ci tels un nom d'utilisateur combiné avec un mot de passe, un jeton cryptographique, un certificat ou une preuve de l'identité jugée pertinente;

7° « Loi » : la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03);

8° « organisme public » : un organisme public au sens de l'article 2 de la Loi;

9° « personne » : une personne physique agissant pour elle-même ou dans le cadre d'une fonction, une entreprise ou une autre entité;

10° « secret partagé » : une information connue seulement d'un organisme public et d'une personne qui entend utiliser ou autrement bénéficier d'un service, lors d'une communication sécurisée. Le secret partagé peut être, par exemple, un mot de passe ou une phrase secrète;

11° « service » : un service d'un organisme public faisant appel aux technologies de l'information, y compris le service offert à l'interne de l'Administration publique.

3. Les présentes règles s'appliquent aux organismes publics visés à l'article 2 de la Loi, lesquels forment l'Administration publique aux fins de la Loi et des présentes règles.

SECTION II
PRINCIPES DIRECTEURS EN IDENTIFICATION ET EN AUTHENTIFICATION

4. Les présentes règles se fondent sur les principes directeurs suivants :

— **Unicité :** Chaque personne est unique. L'unicité permet de distinguer une personne d'une autre et, selon le cas, de l'identifier de façon unique. Une personne détient par conséquent un seul compte pour elle-même et par système d'identification, sans possibilité de partager ou détenir ce compte avec une autre personne;

— **Équivalence des identités :** L'identité d'une personne et l'identité numérique d'une telle personne sont équivalentes. Ces deux identités représentent une personne et ont pour objectif de la reconnaître et de la distinguer d'une autre personne, que les processus pour ce faire s'effectuent en présence de cette personne ou par moyens technologiques;

— **Exactitude :** L'exactitude de l'information confirmant l'identité d'une personne peut notamment être assurée en corroborant cette information auprès d'une source de confiance par application de la loi;

— **Interopérabilité :** Les dispositions prévues aux présentes règles s'inspirent des normes et des standards généralement reconnus au Canada en vue de faciliter l'interopérabilité avec d'autres acteurs de l'écosystème sur le plan national ou international, conformément à la loi;

— **Respect de la vie privée et protection de l'information :** La collecte, l'utilisation, la communication et la conservation de renseignements personnels doivent être effectuées conformément à la loi, notamment la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1). La sécurité de tels renseignements collectés, utilisés, communiqués ou conservés doit être assurée par des mesures de protection appropriées, notamment en considérant la sensibilité de ceux-ci.

SECTION III
ASSURANCE DE L'IDENTITÉ NUMÉRIQUE

§1. Détermination du niveau d'assurance de l'identité

5. Un organisme public doit, pour chaque service sous sa responsabilité, déterminer le niveau d'assurance de l'identité qui est requis pour un tel service, en sélectionnant l'un des quatre niveaux d'assurance de l'identité apparaissant à l'annexe 1. Ces niveaux – faible, moyen, élevé ou très élevé – s'inspirent du Cadre de confiance pancanadien (CCP) du Conseil canadien de l'identification et de l'authentification numériques (CCIAN) et ils correspondent à un besoin de confiance décrit à cette annexe, sous chacun d'eux.

Pour ce faire, un tel organisme doit évaluer le besoin de confiance qui lui est requis pour offrir le service sous sa responsabilité à une personne qui est celle qu'elle prétend être, dans le contexte que toute atteinte à la confidentialité, à la disponibilité et à l'intégrité d'une information pourrait risquer de causer un préjudice à une personne, à un organisme public ou au gouvernement.

L'obligation d'évaluer le besoin visé au deuxième alinéa s'applique pour tous les services qu'offre un organisme public, même si, à la suite de cette évaluation, certains services ne nécessiteront pas l'application des dispositions des sous-sections 2 et 3 de la présente section concernant l'identification et l'authentification, notamment parce que ces services seront offerts à tous ou anonymement.

6. Un organisme public doit s'assurer, lors de la prestation d'un service sous sa responsabilité et en fonction du niveau d'assurance de l'identité déterminé conformément à l'article 5, de l'application de l'identification visée à la sous-section 2 de la section III et, lorsque requis, de l'authentification visée à la sous-section 3 de cette section.

§2. Identification

7. L'identification est un processus de vérification permettant d'identifier, de façon unique, une personne qui entend utiliser ou autrement bénéficier d'un service. Un tel processus peut permettre d'établir l'identité dont une personne se réclame afin de pouvoir avoir accès au service concerné.

8. L'identification est effectuée en s'assurant que le niveau d'assurance de l'identité qui est appliqué dans le cadre d'une demande de service que formule une personne est égal ou supérieur à celui déterminé conformément à l'article 5.

Elle est également effectuée en s'assurant que les exigences liées au niveau d'assurance de l'identité ainsi déterminé, énoncées à l'annexe 2 pour un tel niveau, sont respectées.

§3. Authentification

9. L'authentification est un processus de validation permettant d'assurer que la personne qui entend utiliser ou autrement bénéficier d'un service est bien celle qu'elle prétend être. Elle vise à donner l'assurance qu'une telle personne conserve le contrôle des justificatifs lui permettant l'accès au service concerné et que ceux-ci n'ont pas été compromis.

10. Lors de l'authentification d'une personne qui entend utiliser ou autrement bénéficier d'un service, le niveau d'assurance de l'identité à être appliqué pour le service concerné doit être égal ou supérieur à celui déterminé conformément à l'article 5.

À cette même occasion, il doit également être assuré que les exigences liées au niveau d'assurance de l'identité ainsi déterminé, énoncées à l'annexe 3 pour un tel niveau, sont respectées.

11. Un choix de facteurs d'authentification doit être offert à toute personne qui entend utiliser ou autrement bénéficier d'un service et pour lequel une authentification est requise. Un facteur d'authentification peut, par exemple, prendre la forme d'un jeton, d'un jeton logiciel, de la biométrie ou de tout autre facteur rendu disponible pour le service concerné, dans le respect des exigences liées à l'authentification prévues à la loi et aux présentes règles, dont la nécessité de la collecte des renseignements personnels et du consentement de la personne concernée selon les circonstances.

Des dispositifs supplémentaires à sélectionner doivent également être rendus disponibles pour une telle personne afin de pallier toute perte ou toute défaillance du dispositif primaire d'authentification pour l'authentification multifacteur.

§4. Autres dispositions

12. Les activités liées à l'identification et à l'authentification visées aux sous-sections 2 et 3 de la présente section peuvent être exécutées en régie par l'organisme responsable du service concerné, par un autre organisme public ou par un prestataire de services qui est lié par contrat.

SECTION IV
PREUVE D'IDENTITÉ

13. Lors de l'identification ou de l'authentification d'une personne physique qui entend utiliser ou autrement bénéficier d'un service, une preuve de l'identité essentielle et une preuve de l'identité contextuelle en provenance d'une telle personne peuvent lui être exigées en fonction du niveau d'assurance de l'identité déterminé pour ce service conformément à l'article 5 et pour satisfaire aux exigences qui sont associées à ce niveau.

Lorsqu'une telle personne est représentée par une autre personne physique, une preuve de la capacité d'agir de cette autre personne doit être exigée.

Dans le présent article, on entend par :

« preuve de l'identité essentielle » : l'acte de naissance d'une personne, son certificat ou une copie officielle, une preuve de sa citoyenneté canadienne ou tout autre document officiel émanant d'une autorité étatique, une source considérée fiable, établissant son identité et sa date de naissance;

« preuve de l'identité contextuelle » : une preuve, autre qu'une preuve de l'identité essentielle, mentionnant un attribut de l'identité considéré pertinent pour l'identification.

14. Lors d'une identification ou d'une authentification d'une entreprise ou d'une autre entité, la preuve de son existence et de son identification peut être demandée.

Dans le cas d'une entreprise ou d'une entité autre qu'un organisme public, la preuve visée au premier alinéa peut découler de la consultation du registre prévu à la Loi sur la publicité légale des entreprises (chapitre P-44.1) ainsi que de l'obtention de tout autre document procurant une certitude de son existence et de son identité. Une telle preuve doit également être accompagnée d'un document attestant de la qualité et de la capacité du représentant de cette entreprise ou de cette entité.

Dans le cas où l'entité est un organisme public, la preuve visée au premier alinéa peut découler de la consultation d'un document public tel une loi ou un décret ou de l'obtention d'une déclaration signée par un représentant autorisé en vertu du règlement sur la délégation de signature en vigueur pour un tel organisme ou en vertu de tout autre document équivalent.

15. Les dispositions de la sous-section 2 de la section III concernant l'identification doivent être appliquées au représentant visé à l'un des articles 13 et 14.

16. Le représentant visé au deuxième alinéa de l'article 14 est responsable de la gestion des accès liés au compte d'une entreprise ou d'une entité et il peut autoriser toute autre personne physique œuvrant au sein de cette entreprise ou de cette entité à accéder à ce compte.

SECTION V
VÉRIFICATION DE L'IDENTITÉ PAR UN AGENT

17. L'entité chargée d'une identification peut désigner une personne physique pour agir à titre d'agent aux fins de procéder à une vérification de l'identité d'une personne qui entend utiliser ou autrement bénéficier d'un service.

18. Avant toute désignation d'un agent en vertu de l'article 17, l'entité chargée d'une identification doit s'assurer que la personne à être désignée pour agir à ce titre a suivi une formation portant minimalement sur ces sujets :

1° la protection des renseignements personnels et les lois applicables;

2° la vérification de l'identité;

3° la détection des risques d'atteinte à la confidentialité, à la disponibilité ou à l'intégrité d'une information comme, par exemple, les risques de fraude;

4° la détection des techniques permettant notamment la contrefaçon d'une preuve d'identité et de vidéos.

19. Une vérification de l'identité par un agent peut être effectuée sur place ou à distance, en employant tout moyen qui permet à l'agent de voir et d'entendre la personne physique faisant l'objet d'une telle vérification.

20. Une vérification de l'identité par un agent implique, selon les circonstances et en fonction des exigences prévues à l'annexe 2, une corroboration de l'information obtenue de la personne concernée, et ce, en procédant à une vérification auprès d'une source de confiance, en application de la loi ou conformément à un décret pris en application de l'article 12.14 de la Loi.

21. Une vérification par un agent est obligatoire, en outre des situations prévues en annexe 2, dans les cas suivants :

1° lorsque l'attribut de base ou la preuve de l'identité demandé ne peut être fourni par une personne;

2° après cinq tentatives d'identification sans succès;

3° en cas d'atteinte ou de risque d'atteinte à la confidentialité, à la disponibilité ou à l'intégrité de l'information d'une personne lorsque, par exemple, il y a tentative de fraude ou détection d'une anomalie.

22. La vérification de l'identité d'une personne qui entend utiliser ou autrement bénéficier d'un service peut, en lieu et place de celle effectuée par un agent conformément à la présente section, être exécutée à l'aide d'un moyen technologique, conformément à la loi et aux conditions et modalités d'application prévues dans un cadre pris par le gouvernement ou par le ministre de la Cybersécurité et du Numérique. En ce cas, les articles 19 à 21 s'appliquent avec les adaptations nécessaires.

SECTION VI
FÉDÉRATION

23. Lorsqu'un organisme public entend conclure, conformément à la loi et dans le respect des présentes règles, une entente de collaboration avec une entité offrant un service d'identification ou d'authentification, étant appelée « une fédération », une analyse de risques doit être réalisée préalablement à la conclusion d'une telle entente, y compris notamment une évaluation des facteurs relatifs à la vie privée spécifique à cette fédération.

L'entente visée au premier alinéa doit également stipuler des obligations prévoyant le respect des exigences prévues aux présentes règles ainsi que des niveaux d'assurance de l'identité à être déterminés conformément à l'article 5, lesquels niveaux ne peuvent en aucun cas être inférieurs ou différents de ceux prévus en application de cet article.

L'entente visée au premier alinéa ne peut stipuler que l'organisme public est exonéré en tout ou en partie de toute responsabilité qui lui incombe en vertu de la loi et des présentes règles.

SECTION VII
DISPOSITIONS DIVERSES

24. Un organisme public doit mettre en place un processus permettant de signaler, à un titulaire d'un compte visé par les présentes règles, un accès suspecté non autorisé à ce compte. Un tel processus doit permettre une réponse rapide afin de bloquer tout accès non autorisé et d'invalider les actions qui y sont associées.

Le processus visé au premier alinéa doit également permettre à la personne concernée de reprendre le contrôle du compte créé en son nom propre.

25. Le niveau d'assurance de l'identité déterminé conformément à l'article 5 visant à assurer l'identité d'une personne qui entend utiliser ou autrement bénéficier d'un service doit être maintenu tout au long d'une session. En cas de diminution du niveau d'assurance de l'identité ainsi déterminé en dessous du niveau requis, quelle qu'en soit la raison, la session en cours doit être interrompue.

26. L'entité responsable de l'identification d'une personne doit mettre en place un mécanisme de renouvellement des preuves d'identité fournies par une personne qui entend utiliser ou autrement bénéficier d'un service. Ce renouvellement peut être effectué en validant de nouveau les preuves essentielles de l'identité et les preuves contextuelles de l'identité. Ce renouvellement peut également être effectué de façon automatique par un système, en fonction du niveau d'assurance de l'identité établi conformément à l'article 5.

Le délai maximal de renouvellement visé au premier alinéa, selon le niveau d'assurance de l'identité, est celui apparaissant au tableau suivant :

Alias	Niveau d'assurance de l'identité	Fréquence de renouvellement
ID1	Faible	Non applicable
ID2	Moyen	36 mois
ID3	Élevé	18 mois
ID4	Très élevé	12 mois

Advenant que la validation visée au premier alinéa ne soit pas possible ou qu'un renouvellement n'ait pas été effectué dans le délai prescrit au deuxième alinéa, l'entité responsable de l'identification d'une personne doit soumettre cette personne à une nouvelle identification conformément aux dispositions de la sous-section 2 de la section III lorsqu'une telle personne entend de nouveau utiliser ou autrement bénéficier d'un service.

27. L'entité responsable de l'identification ou de l'authentification d'une personne qui entend utiliser ou autrement bénéficier d'un service doit constituer un registre relatif à ces processus.

Le registre visé au premier alinéa doit notamment comprendre les renseignements concernant un compte, son attribution, sa suspension, sa récupération, sa maintenance, sa révocation et son renouvellement. Ce registre doit être tenu à jour de façon continue et faire l'objet d'une révision annuellement.

28. L'entité responsable de l'identification ou de l'authentification d'une personne qui entend utiliser ou autrement bénéficier d'un service doit, conformément à la loi, utiliser les renseignements personnels d'une telle personne lorsque cela est nécessaire aux fins prévues aux présentes règles, et voir à leur conservation ou à leur destruction de façon sécuritaire.

29. Les dispositions prévues aux présentes règles s'appliquent, avec les adaptations nécessaires, aux identités machine que peut autoriser un organisme public au regard de l'un de ses services.

Pour l'application du présent article, on entend par « identité machine » une clé cryptographique ou un certificat numérique assurant la sécurité des communications, ainsi que des autorisations accordées, entre des actifs informationnels tel que le matériel, un logiciel, une application ou un site Web.

SECTION VIII
DISPOSITIONS DIVERSES, TRANSITOIRES ET FINALES

30. Les présentes règles ne doivent pas être interprétées comme ayant pour effet de modifier ou de remplacer en tout ou en partie la Directive sur les services de certification offerts par le gouvernement du Québec visée par le décret numéro 6-2014 du 15 janvier 2014, laquelle directive continue de s'appliquer, jusqu'à ce qu'elle soit remplacée ou abrogée.

31. Un organisme public peut, à compter de la date d'entrée en vigueur des présentes règles, échelonner la mise en œuvre des mesures permettant l'application de celles-ci sur une période maximale de 36 mois suivant cette date.

32. Les présentes règles remplacent les Orientations et stratégie concernant l'authentification des citoyens et des entreprises dans le cadre du gouvernement électronique, prises par le Conseil du trésor en août 2004.

33. Les présentes règles entrent en vigueur le dixième jour suivant leur publication à la *Gazette officielle du Québec*.

ANNEXE 1
(Article 5)

NIVEAU D'ASSURANCE DE L'IDENTITÉ

Alias	Niveau d'assurance de l'identité	Description du besoin de confiance
ID1	Faible	Besoin d'un niveau faible qu'une personne est celle qu'elle prétend être, et que cette personne a gardé le contrôle des justificatifs qui lui ont été émis et que ceux-ci n'ont pas été compromis.
ID2	Moyen	Besoin d'un niveau moyen qu'une personne est celle qu'elle prétend être et que cette personne a gardé le contrôle des justificatifs qui lui ont été émis et que ceux-ci n'ont pas été compromis.
ID3	Élevé	Besoin d'un niveau élevé qu'une personne est celle qu'elle prétend être et que cette personne a gardé le contrôle des justificatifs qui lui ont été émis et que ceux-ci n'ont pas été compromis.
ID4	Très élevé	Besoin d'un niveau très élevé qu'une personne est celle qu'elle prétend être et que cette personne a gardé le contrôle des justificatifs qui lui ont été émis et que ceux-ci n'ont pas été compromis.

ANNEXE 2
(Articles 8 et 20)

EXIGENCES APPLICABLES AU REGARD DE CHAQUE NIVEAU D'ASSURANCE DE L'IDENTITÉ

Alias	Niveau d'assurance de l'identité	Description du besoin de confiance	Exigences	
			Personnes physiques	Entreprises ou autres entités
VI1	Faible	Besoin d'un niveau faible que la personne est celle qu'elle prétend être.	Autodéclaration (les renseignements ne sont pas vérifiés) et la personne certifie être celle qu'elle prétend être.	
VI2	Moyen	Besoin d'un niveau moyen qu'une personne est celle qu'elle prétend être.	Les attributs de base de l'identité et une preuve de l'identité avec photo, autant que possible corroborés auprès d'une source de confiance (la preuve de l'identité peut être remplacée par deux secrets partagés corroborés).	Les attributs de base de l'entité, une preuve de sa constitution, autant que possible corroborés auprès d'une source de confiance, un secret partagé et un document conférant l'autorité à son représentant. Une vérification de niveau élevé pour ce représentant.
VI3	Élevé	Besoin d'un niveau élevé qu'une personne est celle qu'elle prétend être.	Les attributs de base de l'identité et deux preuves de l'identité (une avec photo et une essentielle), vérifiés par un agent et corroborés auprès d'une source de confiance.	Les attributs de base de l'entité et une preuve de sa constitution corroborés auprès d'une source de confiance, deux secrets partagés et un document conférant l'autorité à son représentant. Une vérification de niveau élevé pour ce représentant.
VI4	Très élevé	Besoin d'un niveau très élevé qu'une personne est celle qu'elle prétend être.	Les attributs de base de l'identité et trois preuves de l'identité (dont deux avec photo et une essentielle), vérifiés par un agent et corroborés auprès d'une source de confiance.	Les attributs de base de l'entité et une preuve de sa constitution corroborés auprès d'une source de confiance, deux secrets partagés et un document notarié conférant l'autorité à son représentant vérifiée par un agent. Une vérification de niveau très élevé pour le représentant.

ANNEXE 3
(Article 10)

NIVEAUX D'ASSURANCE POUR L'AUTHENTIFICATION

Nom	Niveau d'assurance de l'identité	Description du besoin de confiance	Exigences
AU1	Faible	Besoin d'un niveau faible que la personne a gardé le contrôle des justificatifs qui lui ont été émis et que ceux-ci n'ont pas été compromis.	Authentification avec un facteur.
AU2	Moyen	Besoin d'un niveau moyen que la personne a gardé le contrôle des justificatifs qui lui ont été émis et que ceux-ci n'ont pas été compromis.	Authentification multifacteur de base.
AU3	Élevé	Besoin d'un niveau élevé que la personne a gardé le contrôle des justificatifs qui lui ont été émis et que ceux-ci n'ont pas été compromis.	Authentification multifacteur avancée.
AU4	Très élevé	Besoin d'un niveau très élevé que la personne a gardé le contrôle des justificatifs qui lui ont été émis et que ceux-ci n'ont pas été compromis.	Authentification multifacteur avancée, incluant au moins un dispositif cryptographique matériel.

78391