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

*Better government: with partners, for Canadians*

# Solutions technologiques d'authentification électronique (STAE)

# Architecture et spécifications de l'interface (ASI)

# Version 2.0 :

# Profil de déploiement

**État : Version finale r8.2**
**Date de modification : Le 11 juillet, 2018 10:15**
Nom du fichier : TBSSCT-#1045218-v4-CA_-_CATS_IA&S_V2_0_Deployment_Profile_Final_r8_2_en.docx

**Approuvé par :**

Comité des directeurs généraux sur l'authentification électronique

Canada

## Fiche des révisions

| VERSION NO | DESCRIPTION | DATE DE DÉLIVRANCE | ÉTAT | AUTEUR ET REMARQUES |
|---|---|---|---|---|
| Ébauche r8.0 | Texte initial avec des changements marqués en fonction du document CA - CHATS IA&S V2.0_Deployment Profile_Final r7.2_en.doc | 16 février 2012 | Intégration de l'ébauche dans les décisions de la fédération des justificatifs du gouvernement du Canada (FJGC) | Bob Sunday, SCT |
| Ébauche r8.1 | | Pas diffusée | Corrections rédactionnelles seulement | Doug Harris, Services partagés Canada (SPC) |
| Ébauche r8.2 | Mise à jour de base afin de tenir compte de l'état actuel | 8 septembre 2017 | Ébauche pour l'examen des membres de la FJGC | Doug Harris, SPC |
| Version finale r8.2 | Approuvée par le comité des DG sur l'authentification électronique, le 7 févr. 2016 | 20 février 2018 | Approuvée | Doug Harris, SPC |

### Note de lancement pour cette version r8.2

Le présent document « Solutions technologiques d'authentification électronique – Architecture et spécifications de l'interface – Version 2.0 : Profil de déploiement » est une mise à jour du document de base précédent : <<CA - CHATS IA&S V2.0_Deployment Profile_Final r8.0_en.doc> >. Cette version a) met à jour certains documents de référence à leurs plus récentes révisions b) intègre des changements qui ont été appliqués par la FJGC depuis février 2012, et c) corrige des erreurs mineures de rédaction.

Les changements subséquents de ce document de référence continueront d'être traités avec des demandes de changement et des dispositions officielles.

# Table des matières

# INTRODUCTION

## 1.1 Vision de l'initiative d'authentification électronique

L'initiative d'authentification électronique au gouvernement du Canada a une vision qui est partiellement décrite dans le schéma suivant :

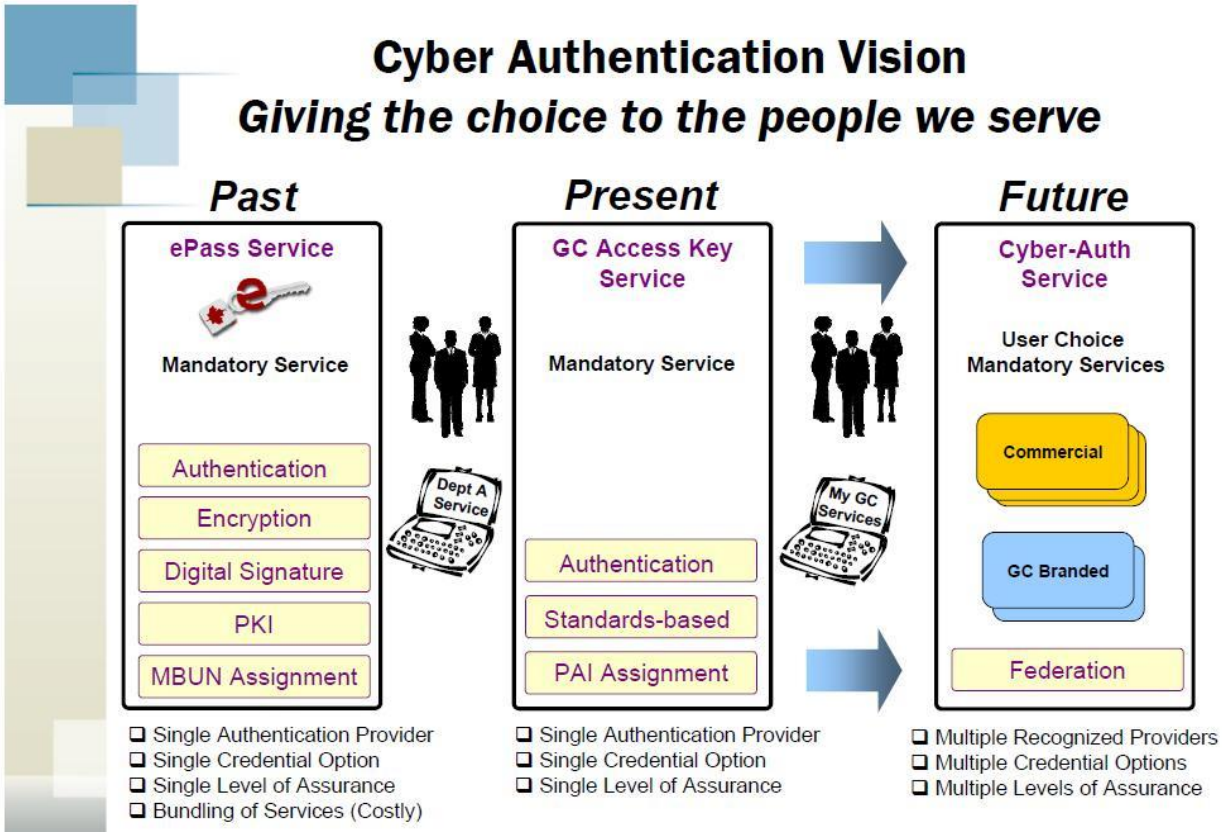


**Figure 1 : Vision d'authentification électronique**

## 1.2 Vue d'ensemble du profil de déploiement de l'ASI des STAE2

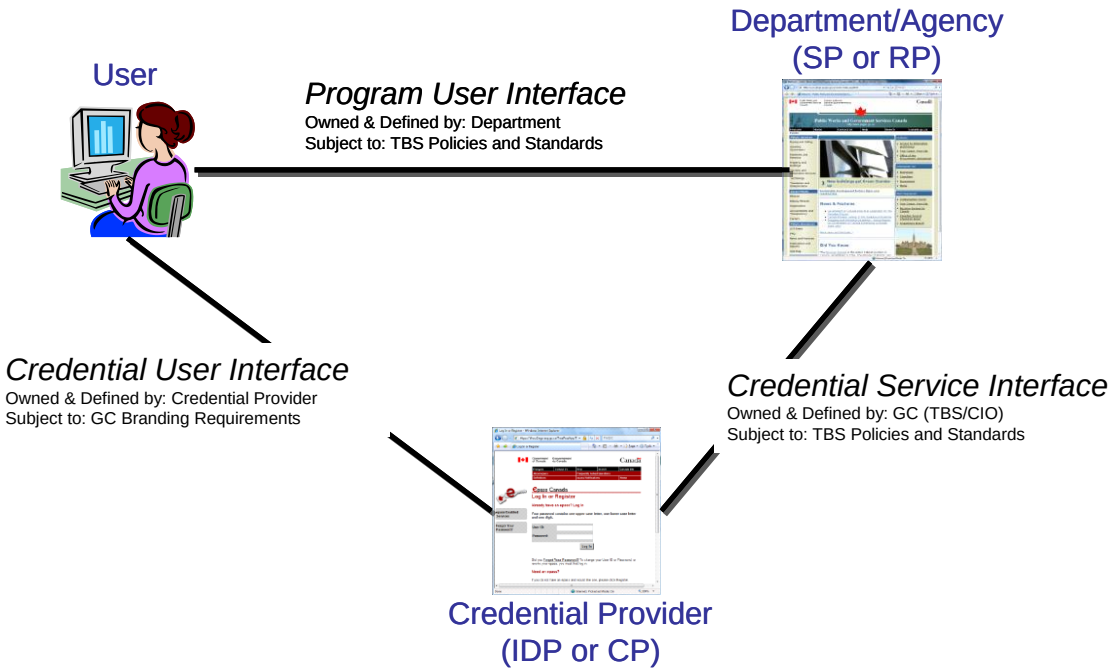


**Figure 2 : Représentation schématisée des interfaces d'authentification**

Ce « *profil de déploiement de l'ASI des STAE2* » [ASI des STAE2] est un profil de niveau de déploiement pour la participation dans l'environnement d'authentification électronique du gouvernement du Canada. Il décrit l'interface de messagerie appelée Interface des services de justificatifs dans la Figure 2. Les autres interfaces illustrées dans le schéma sont définies par le ministère ou organisme ou le fournisseur de justificatifs.

Il s'applique aux déploiements configurés pour participer en tant que fournisseurs de services (FS) et fournisseurs d'identité (FI). Dans le contexte actuel du GC, les FS sont aussi appelés les parties dépendantes (PD), généralement les services électroniques du ministère, et les FI sont appelés fournisseurs de justificatifs d'identité (FJI) ou fournisseurs de services de justificatifs (FSJ). Le GC fait également référence à un service de courtier de justificatifs d'identité (SCJI), qui est une entité de système qui agit à la fois comme un FI pour les PD et comme une PD lorsqu'elle communique avec les FI sous-jacentes; les documents de langage SAML l'appelle Fournisseur d'identité proxy.

*REMARQUE : Dans le présent document, nous utilisons la terminologie de FS et de FI. D'autres documents sur l'authentification électronique peuvent utiliser les termes PD, FJI et FSJ. Les documents de langage SAML et de Kantara Initiative utilisent les termes « FS » et « FI ». Le présent document n'utilise pas le terme « SCJI » puisqu'il s'agit d'une mise en œuvre composite des rôles de FS et de FI.*

*Le présent document utilise les termes « utilisateur », « principal » et « sujet » comme des synonymes.*

Ce profil de déploiement profil est une évolution de l'ancien document du GC « Architecture et spécifications d'interface de la Solution tactique d'authentification électronique (STAE) » [ASI de la STAE] et est une mise à jour de la version finale de r7.2 de [ASI des STAE2].

Ce profil de déploiement n'est ni un didacticiel ni un document d'orientation. La Fédération des justificatifs du gouvernement du Canada (FJGC) peut fournir d'autres conseils et cas d'utilisation.

## 1.3 Conformité au profil de déploiement de l'ASI des STAE2

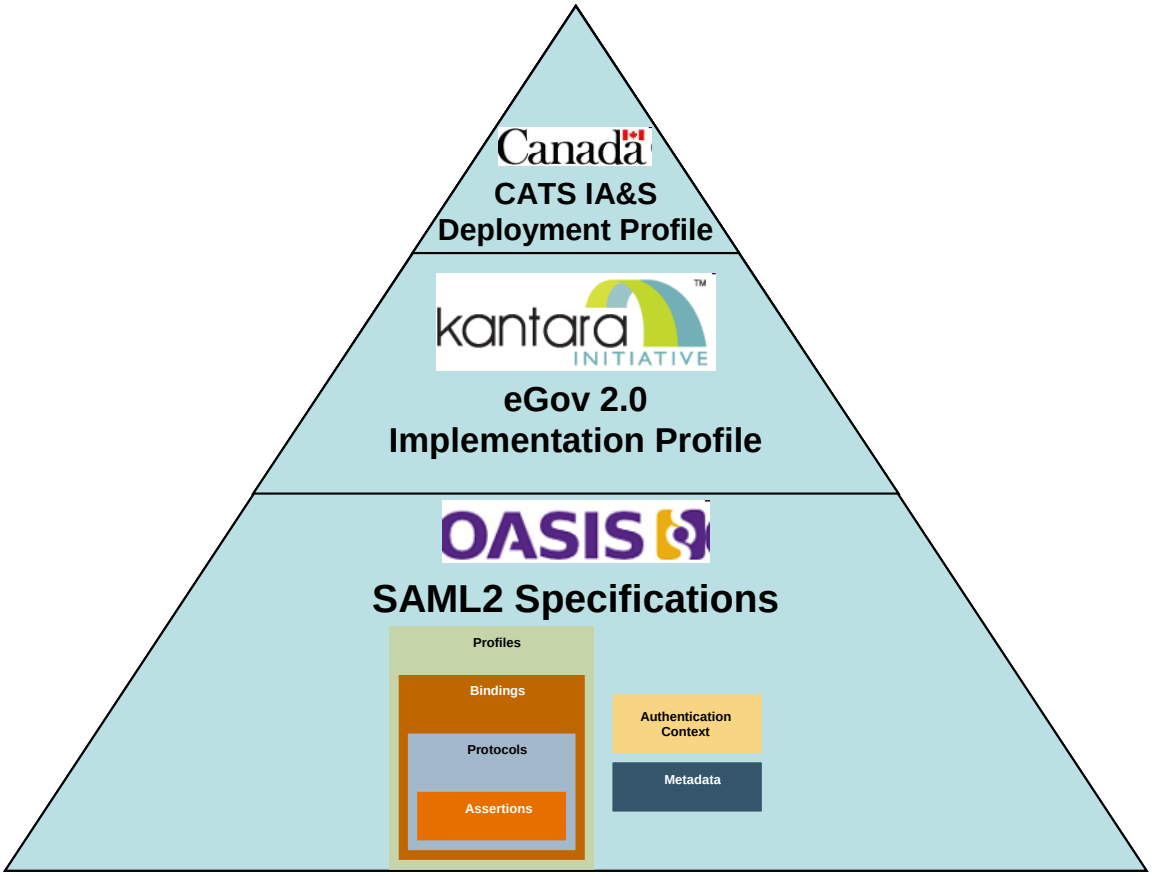


**Figure 3 : L'architecture d'interface de l'authentification électronique Éléments de base**

Ce profil de déploiement repose sur le profile eGov 2.0 [eGov 2.0] publié par Kantara Initiative, mais n'exige pas la conformité complète avec celui-ci. Les exigences normatives de ce profil de déploiement du GC en ce qui concerne les articles pertinents du profil eGov 2.0 sont indiquées en détail dans la section 2 du présent document. Le profil eGov 2.0 est fondé sur les spécifications du langage SAML 2.0 créées par le Comité technique des services de sécurité (CTSS) d'OASIS. Le profil eGov 2.0 limite les fonctions, les éléments, les attributs et les autres valeurs de base de SAML 2.0 nécessaires pour les fédérations et les déploiements approuvés du gouvernement numérique. Sauf indication contraire, les opérations et les fonctions de SAML suivent celles que l'on trouve dans les spécifications SAML 2.0 d'OASIS [SAML2*].

*REMARQUE : Les essais d'interopérabilité effectués par des organismes externes, comme Kantara Initiative, peuvent faciliter la confirmation de la conformité. Par conséquent, les achats du GC qui exigent la conformité avec ce profil de déploiement peuvent aussi exiger que les logiciels sous-jacents pour se conformer aux essais d'interopérabilité externes.*

*Toutefois, ces essais externes ne forment pas une confirmation complète et définitive de la conformité à ces exigences de déploiement du GC. La FJGC peut exiger d'autres essais afin de permettre la participation dans la FJGC.*

### 1.3.1 Notation

Cette spécification utilise un texte normatif pour décrire l'utilisation des capacités du langage SAML.

Les mots-clés « DOIT/DOIVENT », « NE DOIT PAS/NE DOIVENT PAS » « REQUIS/TENU », « DEVRAIT/DEVRAIENT », « NE DEVRAIT PAS/NE DEVRAIENT PAS », « RECOMMANDÉ », « PEUT/PEUVENT » et « FACULTATIF » des présentes spécifications doivent être interprétés conformément à la description qui en est faite dans le document [RFC 2119].

> … ils DOIVENT être utilisés seulement lorsqu'il est réellement nécessaire pour l'interfonctionnement ou pour limiter le comportement qui est capable de causer des préjudices (p. ex., la limitation des retransmissions)…

Par conséquent, on met ces mots clés en majuscules pour indiquer clairement les exigences sur le protocole, les fonctions d'application et le comportement qui touchent l'interopérabilité et la sécurité des mises en œuvre.

## 1.4 Modifications par rapport au document précédent STAE2 de version finale r8.0

Le présent document, [CATS2 IA&S r8.0], diffère de [CATS2 IA&S r8.0] dans un certain nombre de domaines :



Ces modifications sont généralement décrits ci-dessous; les exigences de conformité normatives entièrement détaillées pour ce profil de déploiement sont indiquées dans le présent document, à la section 2 intitulée : « **Error! Reference source not found.** ».

### 1.4.1 Mise à jour des références de document

La section 1.5 a été mise à jour pour tenir compte des documents de référence qui ont été révisés ou remplacés.

### 1.4.2 Un modèle pour l'attribution de valeurs de la FJGC

L'exploitant de la FJGC a publié un document comprenant toutes les valeurs réelles STAE2 et les contraintes qui leur sont attribuées ou prescrites par l'exploitant de la FJGC. Afin d'éviter toute confusion, les valeurs de l'exemple fictif dans le modèle de document ont été supprimées.

### 1.4.3 Exigences en matière de sécurité

Les exigences en matière de sécurité à la section 2.4.5 ont été mises à jour pour tenir compte de l'utilisation interrompue de la version 3 du protocole SSL.

### 1.4.4 De nombreuses corrections et mises à jour diverses

Un certain nombre de corrections et de mises à jour diverses ont été requises :

- Les changements des valeurs de langue de « en » et « fr » à « eng » et « fra » n'étaient que partiellement effectués dans le lancement r8.0. Le changement a été uniformément appliqué à l'ensemble.
- Le texte de la section 2.4.5.1 a été corrigé afin de mieux tenir compte de la décision GCCF-0003 ICM SSL (certificats SSL des Services de gestion des justificatifs internes [GJI]). **Error! Reference source not found.**
- Les références désuètes à Travaux publics et Services gouvernementaux Canada (TPSGC) ont été remplacées par des références à Services partagés Canada (SPC).

## 1.5 Référence des documents

[CATS1 IA&S] « Architecture et spécifications de l'interface de la Solution tactique d'authentification électronique, version 1.0 », en date du 23 janvier 2009

[CATS2 IA&S r7.2] « *Solutions technologiques d'authentification électronique – Architecture et spécifications de l'interface – Version 2.0 : Profil de déploiement* », version finale r7.2, publiée le 25 mars 2011

[CATS2 IA&S r8.0] « *Solutions technologiques d'authentification électronique – Architecture et spécifications de l'interface – Version 2.0 : Profil de déploiement* », ébauche r8.0, publiée le 16 février 2012.

[CATS2 IA&S r8.2] Ce document « *Solutions technologiques d'authentification électronique – Architecture et spécifications de l'interface – Version 2.0 : Profil de déploiement* », ébauche r8.2

[eGov 2.0] « Kantara Initiative eGovernment Implementation Profile of SAML V2.0 Version 2.0 » (en anglais) disponible à l'adresse http://kantarainitiative.org/confluence/download/attachments/42139782/kantara-egov-saml2-profile-2.0.pdf

Glossaire de la FJGC sera produit par la FJGC
Les définitions provisoires se trouvent dans GCpédia à l'adresse http://www.gcpedia.gc.ca/wiki/GC_Credential_Federation/Glossary

[Valeurs de la FJGC] « Fédération des justificatifs du gouvernement du Canada – Valeurs et

contraintes opérationnelles », publié par Services partagés Canada

[ISO 639-2/T] ISO 639-2:1998(E/F), « Codes pour la représentation des noms de langue — Partie 2 : Codes Alpha-3 »
disponible auprès du Conseil canadien des normes (http://www.scc.ca)
http://www.scc.ca

[ITSP.40.111] « Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B », publié par le Centre de la sécurité des télécommunications et disponible à l'adresse
https://www.cse-cst.gc.ca/fr/node/1831/html/26515

[ITSP.40.062] « Conseils sur la configuration sécurisée des protocoles réseau », publié par le Centre de la sécurité des télécommunications et disponible à l'adresse https://www.cse-cst.gc.ca/en/node/1830/html/26507

[ITSP.30.031 V2] « Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information », publié par le Centre de la sécurité des télécommunications et disponible à l'adresse
https://www.cse-cst.gc.ca/fr/node/1842/html/26717

[RFC2119] Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence (en anglais)
http://www.ietf.org/rfc/rfc2119.txt

[SAML2 *] Toutes les références de document SAML2 (en anglais) sont disponibles à l'adresse
http://docs.oasis-open.org/security/saml/v2.0 ou encore à
http://wiki.oasis-open.org/security/FrontPage

[SAML2 Assur] OASIS Committee Specification 01, SAML V2.0 Identity Assurance Profiles Version 1.0, November 2010 (en anglais).
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cs-01.pdf

[SAML2 Bind] Norme OASIS, « Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0 » (en anglais), mars 2005.
http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

[SAML2 Core] Norme OASIS, « Assertions and protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 » (en anglais), mars 2005.
http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SAML2 Errata] OASIS SAML V2.0 errata approuvés (en anglais), le 1er décembre 2009.
http://www.oasis-open.org/committees/download.php/37166/sstc-saml-approved-errata-2.0-02.pdf

[SAML2 Meta] Norme OASIS, « Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 » (en anglais), mars 2005.
http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[SAML2 MetaUI] « OASIS Working Draft 06, Metadata Extensions for Login and Discovery User Interface Version 1.0 » (en anglais), novembre 2010 http://www.oasis-open.org/committees/download.php/40270/sstc-saml-metadata-ui-v1.0-wd06.pdf

[SAML2 Prof] Norme OASIS, « Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 » (en anglais), mars 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

# 2 Exigences de déploiement (normatives)

## 2.1 Restrictions sur le profil eGov 2.0 de Kantara Initiative

Ces spécifications se fondent sur l'ensemble de spécifications du langage SAML 2.0 [SAML2 *] et le profil de SAML2 appelé eGovernment Implementation Profile of SAML2 version 2 (version 2 du Profil de mise en œuvre du gouvernement électronique) de Kantara Initiative [eGov 2.0]

Ce profil de déploiement repose sur conformité complète avec le profil eGov 2.0 [eGov 2.0] publié par Kantara Initiative, mais ne l'exige pas (voir la remarque à la section 1.3 de la page **Error! Reference source not found.** 4). Même si le profil eGov 2.0 de Kantara est un profil de « mise en œuvre » pour les vendeurs de produits logiciels, le profil d'authentification électronique est un profil de « déploiement » plus restreint et explique le déploiement des FS et des FI dans l'environnement d'authentification électronique du GC. Dans les cas où le « Profil de déploiement de l'ASI des STAE2 » ne fournit pas explicitement de consignes propres à la norme SAML2, on DEVRA assurer une mise en œuvre conformément à ce que prévoient les exigences de la norme SAML 2.0 documentées par l'organisme normatif OASIS.

Le tableau qui suit est dans l'ordre et la description des exigences dans [eGov 2.0], les sections 2 et 3, qui sont reprises mot pour mot dans la première colonne. Le tableau est annoté avec le soutien requis par l'Initiative d'authentification électronique du GC : généralement, c'est soit « prise en charge », « limité » ou « s.o. » (sans objet). Chaque fois que d'autres détails sont nécessaires pour expliquer entièrement les exigences du GC, ils sont fournis dans la troisième colonne.

Il y a également des exigences supplémentaires à ces exigences eGov 2.0 et elles sont indiquées dans les sections suivantes. L'authentification électronique a également des restrictions sur les spécifications du langage SAML v2.0 et a quelques exigences particulières liées à l'authentification électronique.

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| eGov 2.2 Gestion des métadonnées et de la confiance | | |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Les mises en œuvre du FI, du FS et du service de découverte DOIVENT prendre en charge l'utilisation des métadonnées du langage SAML v2.0 [SAML2Meta], en conjonction avec leur prise en charge des profils du langage SAML v2.0 indiqués par les sections suivantes. D'autres attentes sur l'utilisation de certains éléments de métadonnées liés au comportement du profil peuvent être satisfaites dans ces sections. | Prise en charge | |
| eGov 2.2.1 Profils de métadonnées | | |
| Les mises en œuvre DOIVENT prendre en charge la version 1 du Profil d'interopérabilité des métadonnées du langage SAML v2.0 [MetaIOP]. | Limitée | Les déploiements de l'authentification électronique NE DOIVENT PAS utiliser la version 1 du Profil d'interopérabilité des métadonnées du langage SAML v2.0 [MetaIOP]. |
| En outre, les mises en œuvre DOIVENT prendre en charge l'utilisation de l'élément <md:KeyDescriptor> comme suit : | Prise en charge | |
| • Les mises en œuvre DOIVENT prendre en charge l'élément <ds:X509Certificate> comme intrant aux exigences subséquentes. La prise en charge pour d'autres représentations clés, et pour d'autres mécanismes de distribution des justificatifs d'identité, est FACULTATIVE. | Limité | Aucun mécanisme FACULTATIF n'est pris en charge. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| • Les mises en œuvre DOIVENT prendre en charge une certaine validation de parcours de la signature, le protocole TLS, et les justificatifs de chiffrement permettant de sécuriser les échanges du langage SAML par rapport à une ou plusieurs autorités de certification de confiance. La prise en charge de PKIX [RFC5280] est RECOMMANDÉE; les mises en œuvre DEVRAIENT consigner le comportement des mécanismes de validation qu'ils utilisent, particulièrement en ce qui concerne les limites ou la divergence de PKIX [RFC5280]. | Prise en charge | Les déploiements de l'authentification électronique DOIVENT respecter les exigences énoncées à la section 2.4.5 Sécurité. |
| • Les mises en œuvre DOIVENT prendre en charge l'utilisation de OCSP [RFC2560] et des listes de révocation de certificats (LRC) obtenues au moyen de l'extension X.509 « CRL Distribution Point » [RFC5280] pour vérifier la révocation de ces justificatifs. | Limitée | Les déploiements de l'authentification électronique DOIVENT respecter les exigences énoncées à la section 2.4.5 Sécurité. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| • Les mises en œuvre PEUVENT prendre en charge des contraintes supplémentaires sur le contenu des certificats utilisés par des entités, comme « subjectAltName » ou « DN », les principales contraintes d'utilisation, ou les élargissements de politique, mais DEVRAIENT consigner ces fonctions et rendre leur activation facultative, dans la mesure du possible. | Limitée | Aucune contrainte supplémentaire FACULTATIVE n'est prise en charge. |
| Veuillez prendre note que ces profils de métadonnées sont destinés à être mutuellement exclusifs dans un contexte de déploiement donné; ce sont des solutions de rechange, plutôt que des utilisations complémentaires ou compatibles de la même information sur les métadonnées. | S.O. | |
| La mise en œuvre DEVRAIT prendre en charge la version 1.0 de l'extension de métadonnées du langage SAML v2.0 pour les attributs d'entité [MetaAttr] et fournir des contrôles de stratégie sur la base des attributs du langage SAML fournis par ce mécanisme d'extension. | Prise en charge | |
| eGov 2.2.2 Échange de métadonnées | | |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Il est FACULTATIF pour les mises en œuvre de prendre en charge la production ou l'exportation de métadonnées, mais les mises en œuvre DOIVENT prendre en charge la publication des métadonnées en utilisant la méthode Well-Known-Location (Emplacement bien connu) définie à la section 4.1 de [SAML2 Meta] (en supposant que les valeurs entityID utilisées conviennent à une telle prise en charge). | Limitée | La FJGC se charge de la gestion et de la distribution des métadonnées actuelles. Pour mettre un terme à l'usage que fait un membre de la Fédération des métadonnées non concurrentes, la FJGC cesse de les distribuer. Elle peut en outre révoquer un certificat du fichier de métadonnées pour des raisons comme l'interruption de la participation d'un membre du regroupement, la mise en péril d'un certificat et des changements des clés.<br>• Les membres de la Fédération DOIVENT soumettre le document des métadonnées XML qui en résulte à la FJGC.<br>• Les membres de la Fédération DOIVENT seulement accepter les documents des métadonnées XML provenant de la FJGC. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Les mises en œuvre DOIVENT prendre en charge les mécanismes suivants pour l'importation des métadonnées.<br>• fichier local;<br>• ressources éloignées à un emplacement fixe accessible au moyen de HTTP 1.1 [RFC2616] ou HTTP 1.1 sur le protocole TLS/SSL [RFC2818].<br>Dans le cas de la résolution HTTP, les mises en œuvre DOIVENT prendre en charge l'utilisation des en-têtes « ETag » et « Last-Modified » pour la gestion du cache. Les mises en œuvre DEVRAIENT prendre en charge l'utilisation de plusieurs emplacements fixes pour l'importation de métadonnées, mais PEUVENT laisser leur comportement inconnu si les métadonnées d'une seule entité se trouvent dans plus d'une source. | Limitée | La FJGC se charge de la gestion et de la distribution des métadonnées actuelles. D'autres procédures seront établies par la FJGC. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| L'importation des métadonnées de plusieurs entités contenues dans un élément <md:EntitiesDescriptor> DOIT être prise en charge. | Limitée | L'importation des métadonnées de plusieurs entités contenues dans un élément <md:EntitiesDescriptor> DEVRAIT être prise en charge.<br>• La FJGC se charge de la gestion et de la distribution des métadonnées actuelles. Au besoin, cette répartition peut être modifiée pour autoriser les logiciels de fournisseur qui ne prennent pas en charge l'importation de métadonnées de plusieurs multiples contenues dans un élément <md:EntitiesDescriptor>. |
| Enfin, les mises en œuvre DEVRAIENT permettre la mise à jour automatique ou la réimportation des métadonnées sans dégradation ou interruption du service. | Prise en charge | |
| eGov 2.2.2.1 Vérification des métadonnées | | |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| La vérification des métadonnées, si prise en charge, DOIT comprendre la vérification des signatures XML au moins au niveau de base de l'élément, et DEVRAIT prendre en charge les mécanismes suivants pour l'établissement clé de la confiance envers les signatures :<br>• Comparaison directe par rapport aux clés connues.<br>• Une certaine forme de validation de certificat fondée sur le chemin par rapport à une ou plusieurs autorités de certificat de confiance, avec les listes de révocation de certificats et/ou OCSP [RFC2560]. La prise en charge de PKIX [RFC5280] est RECOMMANDÉE; les mises en œuvre DEVRAIENT consigner le comportement des mécanismes de validation qu'ils utilisent, particulièrement en ce qui concerne les limites ou la divergence de PKIX [RFC5280]. | Limitée | • Les membres de la Fédération DOIVENT signer leurs métadonnées au moyen du certificat de signature délivré par le service de GJI du GC.<br>• Au moment du traitement, le membre du regroupement s'appuyant sur les métadonnées DOIT vérifier l'état sur le plan de la révocation du certificat ayant servi à signer les métadonnées.<br>o Seules les LRC sont prises en charge. |
| eGov 2.3 Identificateurs de nom | | |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Les mises en œuvre du FI et du FS DOIVENT prendre en charge les formats d'identificateur de nom du langage SAML v2.0, en conjonction avec leur prise en charge des profils du langage SAML v2.0 indiqués par les sections suivantes.<br>• urn:oasis :names:tc:SAML:2.0:nameid-format:persistent<br>• urn:oasis:names:tc:SAML:2.0:nameid-format:transient | Limitée | Les déploiements de l'authentification électronique DOIVENT prendre en charge le format d'identificateur de nom persistant<br>Les déploiements de l'authentification électronique NE DOIVENT PAS prendre en charge le format d'identificateur de nom transitoire. |
| La prise en charge des autres formats est FACULTATIVE. | Limitée | Les déploiements de l'authentification électronique NE DOIVENT PAS prendre en charge les autres formats. |
| eGov 2.4 Attributs | | |
| Les mises en œuvre du FI et du FS DOIVENT prendre en charge la production et la consommation des éléments <saml2:Attribute> qui respectent le profil des attributs X.500/LDAP du langage SAML v2.0 [SAML-X500], en conjonction avec leur prise en charge des profils du langage SAML v2.0 indiqués par les sections suivantes. | Limitée | Les déploiements de l'authentification électronique DOIVENT respecter les exigences énoncées à la section **Error! Reference source not found.Error! Reference source not found.** |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| La capacité de prise en charge des éléments <saml2:AttributeValue> dont les valeurs ne sont pas de simples chaînes (p. ex., <saml2:NameID>, ou autres valeurs XML) est FACULTATIVE. Un tel contenu pourrait être codé base64 comme une solution de rechange. | Limitée | Les déploiements de l'authentification électronique DOIVENT respecter les exigences énoncées à la section **Error! Reference source not found.Error! Reference source not found.** |
| eGov 2.5 Connexion unique de navigateur | | |
| Cette section définit un profil de mise en œuvre du profil SSO de navigateur Web du langage SAML v2.0 [SAML2Prof]. | Prise en charge | |
| eGov 2.5.1 Détection du fournisseur d'identité | | |
| Les mises en œuvre du FS et du service de détection DOIVENT prendre en charge le profil du protocole des services de détection du fournisseur d'identité conformément à la section 2.4.1 de [IDPDisco]. | Limitée | Les déploiements du FI de l'authentification électronique DOIVENT prendre en charge la détection du fournisseur d'identité indiquée dans [SAML2 Prof].<br>Les déploiements du FS de l'authentification électronique PEUVENT prendre en charge la détection du fournisseur d'identité indiquée dans [SAML2 Prof].<br>Les déploiements de l'authentification électronique NE DOIVENT PAS prendre en charge le profil du protocole des services de détection du fournisseur d'identité dans [SAML2 Disco]. |
| eGov 2.5.2 Demandes d'authentification | | |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| eGov 2.5.2.1 Liaison et exigences en matière de sécurité | | |
| Les mises en œuvre du FI et du FS DOIVENT prendre en charge l'utilisation de la liaison de redirection HTTP [SAML2Bind] pour la transmission de messages <saml2p:AuthnRequest>, y compris la production ou la vérification des signatures de concert avec cette liaison. | Prise en charge | |
| La prise en charge pour les autres liaisons est FACULTATIVE. | Limitée | Les déploiements de l'authentification électronique NE DOIVENT PAS prendre en charge les autres liaisons. |
| eGov 2.5.2.2 Contenu du message | | |
| En plus des exigences de la norme de base et celles axées sur le profil, les mises en œuvre du FS DOIVENT prendre en charge l'inclusion des éléments enfants et des attributs <saml2p:AuthnRequest> au moins (le cas échéant) : | Limitée | Tel que précisé ci-dessous. |
| • AssertionConsumerServiceURL | Limitée | Les déploiements de l'authentification électronique NE DEVRAIENT PAS utiliser AssertionConsumerServiceURL.<br>• Le FI obtiendra cela des métadonnées. |
| • ProtocolBinding | Limitée | S'il est présent, l'attribut du paramètre de la liaison du protocole (ProtocolBinding) DOIT correspondre à urn:oasis:names:tc:SAML:2.0:bindings: HTTP-POST. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| • ForceAuthn | Limitée | On PEUT avoir recours au paramètre ForceAuthn pour exiger de la part du FI qu'il impose à l'utilisateur final de s'authentifier à lui quel que soit l'état de la séance d'authentification de l'utilisateur final.<br>• Lorsqu'on utilise le paramètre ForceAuthn, le FS DOIT veiller à ce que le principal ne change pas son ID de nom (NameID) de toute authentification précédente dans la séance, même si elle a expirée.<br>• Si l'on utilise le paramètre ForceAuthn et que l'authentification réussit, cela réinitialisera le paramètre AuthnInstant des FI pour ce principal. |
| • IsPassive | Limitée | • Le paramètre IsPassive peut être utilisé si le FS ne souhaite pas que le FI prenne directement le contrôle du navigateur de l'utilisateur final (c'est-à-dire, qu'il présente une page à l'utilisateur final).<br>• Si la valeur du paramètre IsPassive est « vrai » (« True »), l'utilisateur final DOIT être en mesure d'authentifier d'une manière passive quelconque, à défaut de quoi la réponse obtenue NE DOIT PAS contenir une <assertion>.<br>• Cette fonction permet au FS de déterminer si elle devrait signifier à l'utilisateur final qu'il est sur le point d'interagir avec le FI. Voici un exemple d'une situation passive : le FS découvre au moyen du témoin du domaine commun que l'utilisateur final peut avoir une séance à un FI particulier. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| • AttributeConsumingServiceIndex | Limitée | Les déploiements de l'authentification électronique NE DOIVENT PAS indiquer le paramètre AttributeConsumingServiceIndex. |
| • <saml2p:RequestedAuthnContext> | Limitée | • La demande d'authentification DOIT comprendre le paramètre <RequestedAuthnContext>.<br>• Le paramètre <RequestedAuthnContext> DOIT comprendre un niveau d'assurance comme indiqué dans [SAML2 Assur]. Les niveaux d'assurance (NA) de l'authentification électronique du GC sont définis à la section 2.4.2 Niveaux d'assurance de l'authentification électronique du GC.<br>• Les FS DOIVENT demander un niveau précis d'assurance avec l'opérateur de comparaison « exacte ».<br>• Le SP PEUT demander plusieurs niveaux d'assurance en ordre de priorité. Par exemple, cela est utile lorsqu'un niveau 2 est nécessaire, mais le SP est disposé à accepter un niveau 3 si un niveau 2 n'est pas possible. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| • <saml2p:NameIDPolicy> | Limitée | • Le paramètre <SPNameQualifier> peut être présent.<br>o La FJGC peut constituer des groupes d'affiliation des FS de la FJGC qui utiliseront un identificateur anonyme, persistant (IAP) et commun. Dans ce cas, les FS peuvent utiliser le paramètre <SPNameQualifier> dans la demande d'authentification pour indiquer leur désir pour cet IAP commun.<br>• Le paramètre <NameIDPolicy> PEUT contenir un attribut « AllowCreate ».<br>o En général, l'attribut AllowCreate est réglé de manière à ce qu'il soit « vrai » de sorte que si l'utilisateur final n'a jamais eu recours au FI sélectionné pour accéder au FS, un identificateur d'utilisateur final peut être créé, des messages SAML pouvant être échangés entre les parties.<br>o Toutefois, l'attribut AllowCreate établi à « faux » peut être utile si le FS souhaite désactiver les circuits d'enregistrement de justificatifs dans l'interface utilisateur au FS.<br>• Si le paramètre Format est présent, il DOIT correspondre à urn:oasis:names:tc:SAML:2.0:nameidformat:persistent. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Les mises en œuvre du FI DOIVENT prendre en charge tous les éléments enfants du paramètre <saml2p:AuthnRequest> et les attributs définis par [SAML2Core], mais PEUVENT fournir cette prise en charge en retournant les erreurs appropriées si confrontées par des options de demande particulière. Toutefois, les mises en œuvre DOIVENT pleinement prendre en charge les options énumérées ci-dessus, et être configurables pour utiliser ces options de façon utile comme défini par [SAML2Core]. | Prise en charge | |
| Les mises en œuvre PEUVENT limiter leur prise en charge de l'élément <saml2p:RequestedAuthnContext> à la valeur « exacte » pour l'attribut de comparaison, mais DOIVENT autrement prendre en charge tout contenu admissible de l'élément. | Limitée | Les déploiements de l'authentification électronique DOIVENT seulement prendre en charge la valeur « exacte » pour l'attribut de comparaison. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Les mises en œuvre du FI DOIVENT prendre en charge la vérification des emplacements AssertionConsumerServiceURL demandés au moyen de la comparaison aux éléments <md:AssertionConsumerService> fournis au moyen des métadonnées à l'aide de la comparaison de chaînes sensibles à la casse. La prise en charge d'autres moyens de comparaison ou de mécanismes de vérification de rechange est FACULTATIVE (p. ex., canonicalisation ou autre manipulation des valeurs URL). | Limitée | Les déploiements de l'authentification électronique NE DOIVENT PAS prendre en charge d'autres moyens de comparaison. |
| eGov 2.5.3 Réponses | | |
| eGov 2.5.3.1 Liaison et exigences en matière de sécurité | | |
| Les mises en œuvre du FI et du FS DOIVENT prendre en charge l'utilisation des liaisons HTTP-POST et HTTP-Artifact [SAML2Bind] pour la transmission des messages <saml2p:AuthnRequest>. | Limitée | Les déploiements de l'authentification électronique DOIVENT prendre en charge les liaisons HTTP POST.<br>Les déploiements de l'authentification électronique NE DOIVENT PAS prendre en charge les liaisons HTTP Artifact. |
| La prise en charge pour d'autres liaisons, et pour d'autres types d'artéfacts que urn:oasis:names:tc:SAML:2.0:artifact-04 est FACULTATIVE. | Limitée | Les déploiements de l'authentification électronique NE DOIVENT PAS prendre en charge d'autres liaisons. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Les mises en œuvre du FI et du FS DOIVENT prendre en charge la production et la consommation de messages non sollicités <saml2p:Response> (c'est-à-dire, les réponses qui ne sont pas le résultat d'un message <saml2p:AuthnRequest>). | Limitée | Les déploiements de l'authentification électronique DOIVENT ignorer les messages non sollicités <saml2p:Response>.<br>• On n'a trouvé aucun cas d'utilisation de l'authentification électronique qui exige ceux-ci. |
| Les mises en œuvre du FI DOIVENT prendre en charge l'émission des messages <saml2p:Response> (avec les codes d'état appropriés) en cas d'erreur, pourvu que l'agent utilisateur reste disponible et qu'un emplacement acceptable de livraison de la réponse soit disponible. Les critères d'« acceptabilité » d'un emplacement de réponse ne sont pas officiellement indiqués, mais sont assujettis à la politique du fournisseur d'identité et tiennent compte de sa responsabilité pour protéger les utilisateurs d'être envoyés à des parties non fiables ou peut-être malveillantes. Veuillez noter qu'il s'agit d'une exigence plus solide que le langage comparable dans [SAML2Prof]. | Prise en charge | La FJGC définit l'« acceptabilité d'un emplacement de réponse » pour désigner les métadonnées enregistrées. <AssertionConsumerServiceURL> |
| Les mises en œuvre du FI et du FS DOIVENT prendre en charge la signature des éléments <saml2:Assertion> dans les réponses; la prise en charge de la signature de l'élément <saml2p:Response> est FACULTATIVE. | Limitée | Les déploiements NE DOIVENT PAS prendre en charge la signature de l'élément <saml2p:Response>. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Les mises en œuvre du FI et du FS DOIVENT prendre en charge l'utilisation du chiffrement XML au moyen de l'élément <saml2:EncryptedAssertion> à l'utilisation de la liaison HTTP-POST; la prise en charge des éléments <saml2:EncryptedID> et <saml2:EncryptedAttribute> est FACULTATIVE. | Limitée | Les déploiements de l'authentification électronique NE DOIVENT PAS déployer une prise en charge FACULTATIVE. |
| eGov 2.5.3.2 Contenu du message | | |
| Le profil SSO du navigateur Web permet aux réponses de contenir un certain nombre d'affirmations et d'énoncés. Les mises en œuvre du FI DOIVENT permettre de limiter le nombre d'éléments <saml2:Assertion>, <saml2:AuthnStatement> et <saml2:AttributeStatement> à un dans le message <saml2p:Response>. À son tour, les mises en œuvre du FS PEUVENT limiter la prise en charge à une seule instance de ces éléments au traitement des messages <saml2p:Response>. | Limitée | Les déploiements de l'authentification électronique DOIVENT seulement envoyer des messages <saml2p:Response> contenant au plus un seul élément <saml2:Assertion>. |
| Les mises en œuvre du FI DOIVENT prendre en charge l'inclusion d'un attribut de consentement dans les messages <saml2p:Response>, et un attribut SessionIndex dans les éléments <saml2:AuthnStatement>. | Limitée | Les déploiements du FI de l'authentification électronique NE DOIVENT PAS inclure un attribut de consentement dans les messages <saml2p:Response>.<br>• On n'a trouvé aucun cas d'utilisation de l'authentification électronique qui exige celui-ci. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Les mises en œuvre du FS qui offrent une certaine forme de sémantique de séance DOIVENT prendre en charge l'attribut SessionNotOnOrAfter de l'élément <saml2:AuthnStatement>. | Prise en charge | Voir la section 2.2 pour des contraintes sur les déploiements du FI de l'authentification électronique. |
| Les mises en œuvre du FS DOIVENT prendre en charge l'acceptation ou le rejet d'affirmations en fonction du contenu de l'élément <saml2:AuthnContext> de l'élément <saml2:AuthnStatement>. Les mises en œuvre DOIVENT également prendre en charge l'acceptation ou le rejet d'un contenu particulier <saml2:AuthnContext> en fonction de l'identité du FI. L'[IAP] fournit un tel mécanisme au moyen des métadonnées SAML v2.0 et est RECOMMANDÉ; si cette spécification est sous forme d'ébauche, on ne s'attend pas à ce que les détails techniques changent avant l'approbation éventuelle. | Prise en charge | |
| eGov 2.5.4 Résolution des artéfacts | | |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Conformément à l'exigence énoncée dans la section 2.5.3.1 pour la prise en charge de la liaison HTTP-Artifact [SAML2Bind] pour la transmission de messages <saml2p:Response>, les mises en œuvre DOIVENT prendre en charge le profil de résolution des artéfacts SAML v2.0 [SAML2Prof] comme limité par les sous-sections suivantes. | Limitée | Les déploiements de l'authentification électronique NE DOIVENT PAS prendre en charge la liaison HTTP-Artifact. |
| eGov 2.5.4.1 Demandes de résolution des artéfacts | | |
| Les mises en œuvre du FI et du FS DOIVENT prendre en charge l'utilisation de la liaison SAML SOAP (utilisant HTTP comme transport) [SAML2Bind] pour la transmission des messages <saml2p:ArtifactResolve>. | S.O. | |
| Les mises en œuvre DOIVENT prendre en charge l'utilisation des signatures de message SAML et l'authentification du serveur TLS pour authentifier les demandes; la prise en charge de l'authentification du client TLS, ou d'autres formes d'authentification en conjonction avec la liaison SAML SOAP, est FACULTATIVE. | S.O. | |
| eGov 2.5.4.2 Réponses de résolution des artéfacts | | |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Les mises en œuvre du FI et du FS DOIVENT prendre en charge l'utilisation de la liaison SAML SOAP (utilisant HTTP comme transport) [SAML2Bind] pour la transmission des messages <saml2p:ArtifactResponse>. | S.O. | |
| Les mises en œuvre DOIVENT prendre en charge l'utilisation des signatures de message SAML et l'authentification du serveur TLS pour authentifier les réponses; la prise en charge de l'authentification du client TLS, ou d'autres formes d'authentification en conjonction avec la liaison SAML SOAP, est FACULTATIVE. | S.O. | |
| eGov 2.6 Connexion unique du détenteur de clé du navigateur | | |
| Cette section définit un profil de mise en œuvre de la version 1.0 du profil SSO de navigateur Web du détenteur de clé SAML v2.0 [HoKSSO]. | Limitée | Les déploiements de l'authentification électronique NE DOIVENT PAS prendre en charge. |
| Les exigences en matière de mise en œuvre définies à la section 2.5 pour le profil de non-détenteur de clé s'appliquent aux mises en œuvre de ce profil. | S.O. | |
| eGov 2.7 Mandataire SAML 2.0 | | |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| La section 3.4.1.5 de [SAML2Core] définit une approche formalisée pour établir un protocole mandataire SAML 2.0 de demande d'authentification entre plusieurs FI. Cette section définit un profil de mise en œuvre pour ce comportement approprié pour la composition avec les profils de connexion unique indiqués dans les sections 2.5 et 2.6. | Prise en charge | Les déploiements de l'authentification électronique DOIVENT prendre en charge lorsque configurés de manière à fonctionner comme un FI mandataire. |
| Les exigences du profil sont imposées sur les mises en œuvre du FI agissant comme un mandataire. Ces exigences sont complémentaires aux exigences techniques énoncées dans la section 3.4.1.5.1 [SAML2Core], qui DOIVENT aussi être prises en charge. | Prise en charge | Les déploiements de l'authentification électronique DOIVENT prendre en charge lorsque configurés de manière à fonctionner comme un FI mandataire. |
| eGov 2.7.1 Demandes d'authentification | | |
| Les mises en œuvre du FI mandataire DOIVENT prendre en charge le mappage des éléments <saml2p:RequestedAuthnContext> et <saml2p:NameIDPolicy> de l'entrée à la sortie, de sorte que les agents de déploiement peuvent choisir de transmettre les valeurs ou d'effectuer un mappage entre divers vocabulaires, au besoin. | Prise en charge | Les déploiements de l'authentification électronique DOIVENT prendre en charge lorsque configurés de manière à fonctionner comme un FI mandataire. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Les mises en œuvre du FI mandataire DOIVENT prendre en charge la suppression ou l'omission des éléments <saml2p:RequesterID> des messages <saml2p:AuthnRequest> sortants pour permettre de cacher l'identité du FS des FI mandataire. | Prise en charge | Les déploiements de l'authentification électronique DOIVENT prendre en charge lorsque configurés de manière à fonctionner comme un FI mandataire. |
| eGov 2.7.2 Réponses | | |
| Les mises en œuvre du FI mandataire DOIVENT prendre en charge le mappage des éléments <saml2:AuthnContext> sortants, de sorte que les agents de déploiement peuvent choisir de transmettre les valeurs ou d'effectuer un mappage entre divers vocabulaires, au besoin. | Prise en charge | Les déploiements de l'authentification électronique DOIVENT prendre en charge lorsque configurés de manière à fonctionner comme un FI mandataire. |
| Les mises en œuvre du FI mandataire DOIVENT prendre en charge la suppression des éléments <saml2:AuthenticatingAuthority> des messages <saml2p:AuthnContext> sortants pour permettre de cacher l'identité du FI mandataire des FS. | Prise en charge | Les déploiements de l'authentification électronique DOIVENT prendre en charge lorsque configurés de manière à fonctionner comme un FI mandataire. |
| eGov 2.8 Déconnexion unique | | |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Cette section définit un profil de mise en œuvre du profil de déconnexion unique SAML v2.0 [SAML2Prof].<br>Aux fins de clarification, les exigences techniques pour chaque type de message ci-dessous reflètent l'intention de demander de façon normative le lancement de la déconnexion par un FS en utilisant le canal avant ou arrière, et le lancement ou la propagation de déconnexion par un FI à l'aide du canal arrière. | Prise en charge | |
| eGov 2.8.1 Demandes de déconnexion | | |
| eGov 2.8.1.1 Liaison et exigences en matière de sécurité | | |
| Les mises en œuvre du FI DOIVENT prendre en charge la liaison SAML SOAP (utilisant HTTP comme moyen de transport) [SAML2Bind] aux fins de la délivrance des messages <saml2p:LogoutRequest>, et DOIVENT prendre en charge les liaisons SAML SAVON (utilisant HTTP comme moyen de transport) et HTTP-Redirect [SAML2Bind] pour la réception des messages <saml2p:LogoutRequest>. | Prise en charge | |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Les mises en œuvre du FS DOIVENT prendre en charge la liaison SAML SOAP (utilisant HTTP comme moyen de transport) [SAML2Bind] aux fins de la délivrance et de la réception des messages <saml2p:LogoutRequest>. | Prise en charge | |
| La prise en charge pour les autres liaisons est FACULTATIVE. | Limitée | Les déploiements de l'authentification électronique PEUVENT prendre en charge les liaisons HTTP Redirect pour la délivrance des messages <saml2p:LogoutRequest>.<br>Aucune autre liaison n'est prise en charge. |
| Les mises en œuvre DOIVENT prendre en charge l'utilisation des signatures de message SAML et l'authentification du serveur TLS pour authentifier les messages <saml2p:LogoutRequest>; la prise en charge de l'authentification du client TLS, ou d'autres formes d'authentification en conjonction avec la liaison SAML SOAP, est FACULTATIVE. | Limitée | Les déploiements de l'authentification électronique DOIVENT respecter les exigences énoncées à la section 2.4.5 Sécurité. |
| Les mises en œuvre du FI et du FS DOIVENT prendre en charge l'utilisation du chiffrement XML au moyen de l'élément <saml2:EncryptedID> à l'utilisation de la liaison HTTP-Redirect. | Prise en charge | |
| eGov 2.8.1.2 Comportement de l'interface utilisateur | | |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Les mises en œuvre du FI DOIVENT prendre en charge la résiliation de la séance locale lancée par l'utilisateur seulement et la déconnexion unique lancée par l'utilisateur. À la réception d'un message <saml2p:LogoutRequest> au moyen d'une liaison par canal avant, les mises en œuvre du FI DOIVENT prendre en charge l'intervention de l'utilisateur régissant le choix de propager la déconnexion aux autres FS, ou limitant l'exploitation au FI. Bien sûr, les mises en œuvre DOIVENT retourner les renseignements sur l'état à l'entité qui présente la demande (p. ex., indication de déconnexion partielle), le cas échéant. | Limitée | Les déploiements de l'authentification électronique NE DOIVENT PAS prendre en charge l'intervention de l'utilisateur régissant le choix de propager la déconnexion aux autres FS, ou limitant l'exploitation au FI.<br>• En tout temps, une seule demande de déconnexion produira la déconnexion globale pour la séance du principal. |
| Les mises en œuvre du FS DOIVENT prendre en charge la résiliation de la séance locale lancée par l'utilisateur seulement et la déconnexion unique lancée par l'utilisateur. | Limitée | Les déploiements du FS de l'authentification électronique PEUVENT seulement prendre en charge une déconnexion unique (c'est-à-dire, déconnexion).<br>• Les déploiements du FI de l'authentification électronique DOIVENT propager la déconnexion sans l'intervention de l'utilisateur à tous les FS en cause dans la séance et répondre aux FS d'origine. |
| Les mises en œuvre du FI DOIVENT également prendre en charge le lancement administratif de la déconnexion unique pour toute séance active, sous réserve des politiques appropriées. | Prise en charge | La FJGC indiquera, pour chaque déploiement du FI de l'authentification électronique, la prise en charge, le cas échéant, du lancement administratif de déconnexion unique est nécessaire. |
| eGov 2.8.2 Réponses de déconnexion | | |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| eGov 2.8.2.1 Liaison et exigences en matière de sécurité | | |
| Les mises en œuvre du FI DOIVENT prendre en charge la liaison SAML SOAP (utilisant HTTP comme moyen de transport) [SAML2Bind] aux fins de la délivrance des messages <saml2p:LogoutResponse>, et DOIVENT prendre en charge les liaisons SAML SAVON (utilisant HTTP comme moyen de transport) et HTTP-Redirect [SAML2Bind] pour la réception des messages <saml2p:LogoutResponse>. | Limitée | • Remarque : Les liaisons HTTP Redirect pour la délivrance des messages <saml2p:LogoutResponse> sont dépréciées et DEVRAIT SEULEMENT être utilisées si le message <saml2p:LogoutRequest> a été envoyé à l'aide de cette liaison. |
| Les mises en œuvre du FS DOIVENT prendre en charge la liaison SAML SOAP (utilisant HTTP comme moyen de transport) [SAML2 Bind] aux fins de la délivrance et de la réception des messages <saml2p:LogoutResponse>. | Prise en charge | |
| La prise en charge pour les autres liaisons est FACULTATIVE. | Limitée | Les déploiements de l'authentification électronique NE DOIVENT PAS déployer une prise en charge FACULTATIVE. |
| Les mises en œuvre DOIVENT prendre en charge l'utilisation des signatures de message SAML et l'authentification du serveur TLS pour authentifier les messages <saml2p:LogoutResponse>; la prise en charge de l'authentification du client TLS, ou d'autres formes d'authentification en conjonction avec la liaison SAML SOAP, est FACULTATIVE. | Limitée | Les déploiements de l'authentification électronique NE DOIVENT PAS déployer une prise en charge FACULTATIVE. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| eGov 3 Catégories de conformité | | |
| eGov 3.1 Norme | | |
| Les mises en œuvre conformes des FI et/ou des FS DOIVENT prendre en charge les exigences normatives dans les sections 2.2, 2.3, 2.4 et 2.5. | Prise en charge | |
| eGov 3.1.1 Signatures et algorithmes de chiffrement | | |
| Les mises en œuvre DOIVENT prendre en charge la signature et assimiler les algorithmes indiqués par les adresses URL suivantes en conjonction avec la création et la vérification des signatures XML [XMLSig] :<br>• http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 (indiqué dans [RFC4051])<br>• http://www.w3.org/2001/04/xmlenc#sha256 (indiqué dans [XMLEnc]) | Prise en charge | Cette exigence s'étend aux algorithmes utilisés pour la signature des messages SAML codés URL comme indiqué à la section 3.4.4.1 de [SAML-Bindings]. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Les mises en œuvre DEVRAIENT prendre en charge la signature et assimiler les algorithmes indiqués par les adresses URL suivantes en conjonction avec la création et la vérification des signatures XML [XMLSig] :<br>• http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256<br>(indiqué dans [RFC4051]) | Prise en charge | |
| Les mises en œuvre DOIVENT prendre en charge les algorithmes de chiffrement en blocs indiqués par les adresses URL suivantes en conjonction avec le chiffrement XML [XMLEnc] :<br>• http://www.w3.org/2001/04/xmlenc#tripledes-cbc<br>• http://www.w3.org/2001/04/xmlenc#aes128-cbc<br>• http://www.w3.org/2001/04/xmlenc#aes256-cbc | Prise en charge | Les algorithmes utilisés DOIVENT être des algorithmes cryptographiques approuvés par le Centre de la sécurité des télécommunications Canada (CSTC) pour le chiffrement, comme documenté dans [ITSP.40.111]. |
| Les mises en œuvre DOIVENT prendre en charge les algorithmes de transport de clé indiqués par les adresses URL suivantes en conjonction avec le chiffrement XML [XMLEnc] :<br>• http://www.w3.org/2001/04/xmlenc#rsa-1_5<br>• http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p | Prise en charge | Les algorithmes utilisés DOIVENT être des modèles d'établissement de clés cryptographiques approuvés par le CSTC, comme documenté dans [ITSP.40.111]. |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Les mises en œuvre DEVRAIENT prendre en charge les algorithmes de contrat de clé indiqués par les adresses URL suivantes en conjonction avec le chiffrement XML [XMLEnc] :<br>• http://www.w3.org/2009/xmlenc11#ECDH-ES (indiqué dans [XMLEnc11])<br>(Il s'agit de la dernière version d'ébauche de travail de chiffrement XML 1.1, et cette exigence normative est conditionnelle à la ratification W3C de cette spécification sans changements normatifs à la définition de cet algorithme.) | Prise en charge | Les algorithmes utilisés DOIVENT être des modèles d'établissement de clés cryptographiques approuvés par le CSTC, comme documenté dans [ITSP.40.111]. |
| La prise en charge pour les autres algorithmes est FACULTATIVE. | Limitée | Les déploiements de l'authentification électronique NE DOIVENT PAS prendre en charge d'autres algorithmes. |
| eGov 3.2 Norme avec déconnexion | | |
| Les mises en œuvre conformes des FI et/ou des FS DOIVENT respecter les exigences de conformité à la section 3.1, et DOIVENT en outre prendre en charge les exigences normatives à la section 2.8. | Limitée | Voir la section 2.8 ci-dessus. |
| eGov 3.3 Complet | | |

| eGov 2.0 | ASI des STAE Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Les mises en œuvre conformes des FI et/ou des FS DOIVENT respecter les exigences de conformité à la section 3.1, et DOIVENT en outre prendre en charge les exigences normatives dans les sections 2.6, 2.7 et 2.8. | Limitée | • Les déploiements de l'authentification numérique NE DOIVENT PAS être configurés de manière à respecter la section 2.6.<br>• Les déploiements de l'authentification électronique DOIVENT être configurés pour respecter la section 2.7 si configurés de manière à fonctionner comme un FI mandataire. |
| Fin du tableau | | |

## 2.2 Autres contraintes sur les spécifications [SAML2 *]

En plus des contraintes imposées par ce profil de déploiement sur le profil eGov 2.0 [eGov 2.0] publié par Kantara Initiative, ce document sur les exigences de déploiement de l'authentification électronique impose également certaines contraintes supplémentaires sur les spécifications sous-jacentes SAML 2.0 publiées par le Comité technique des services de sécurité (CTSS) d'OASIS.

| SAML2 * | ASI des STAE<br>Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| [SAML2 Core]<br>Section 2.7.2, ligne 1061<br>`<SessionNotOnOrAfter>` | Limitée | Les déploiements du FI de l'authentification électronique NE DEVRAIENT PAS indiquer l'attribut SessionNotOnOrAfter. Cela permet au FS de choisir sa propre durée requise pour son contexte de sécurité.<br>• Si un FI de la FJGC est incapable de configurer cette valeur pour ne pas être envoyé, il DOIT établir cette valeur à une valeur élevée, comme déterminé par la FJGC. |
| [SAML2 Core]<br>Section 3.2.1, ligne 1489<br>`<saml:Issuer>` | Limitée | Demande d'authentification du FS <saml:Issuer><br>• DOIT être présent<br>• DOIT être l'ID d'entité attribuée par la FJGC. |
| [SAML2 Core]<br>Section 3.4.1, ligne 2017<br>`<saml:Subject>` | Limitée | La demande d'authentification du FS `<saml:Subject>` NE DOIT pas être incluse.<br>• Aucun cas d'utilisation de l'authentification électronique n'exige l'élément `<saml:Subject>`. |

| SAML2 * | ASI des STAE<br>Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| [SAML2 Core]<br>Section 3.4.1, ligne 2029<br><saml:Conditions> | Limitée | La demande d'authentification du FS <saml:Conditions> NE DOIT pas être incluse.<br>• Aucun cas d'utilisation de l'authentification électronique n'exige l'élément <saml:Conditions>. |
| [SAML2 Core]<br>Section 3.4.1, ligne 2068<br>ProtocolBinding | Limitée | Demande d'authentification du FS ProtocolBinding.<br>• PEUT être utilisée.<br>• Si ProtocolBinding est présent, il DOIT être « urn:oasis :names:tc:SAML:2.0:bindings :HTTP-POST ». |
| [SAML2 Core]<br>Section 3.6.1, ligne 2421<br><ManageNameIDRequest> | Limitée | Les déploiements du FI DOIVENT envoyer en temps opportun un paramètre <ManageNameIDRequest> avec un paramètre <Terminate> pour un justificatif d'identité qui a été révoqué à n'importe quel FS qui a un point terminal défini pour le paramètre <ManageNameIDService> et pour lequel il a déjà envoyé une affirmation pour le principal.<br>Les déploiements du FI NE DOIVENT PAS envoyer d'autres messages <ManageNameIDRequest>.<br>Les déploiements du FS DOIVENT répondre aux messages <ManageNameIDRequest>. |

| SAML2 * | ASI des STAE<br>Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| [SAML2 Bind]<br>Section 3.5.3, ligne 785<br><RelayState> | Limitée | Le paramètre <RelayState> PEUT NE PAS être inclus dans un message de réponse, à moins qu'il n'ait été fourni dans un message de demande correspondant. |
| [SAML2 Assur]<br>Section 3, ligne 276<br><assurance-certification> | Limitée | Les métadonnées des FI de l'authentification électronique DOIVENT indiquer les niveaux d'assurance pris en charge dans l'attribut e <assurance-certification> comme indiqué dans [SAML2 Assur], Section 3 Profil des attributs de certification d'assurance de l'identité<br>Les valeurs d'URL qui seront utilisées dans les quatre niveaux d'assurance sont indiquées à la section 2.4.2 Niveaux d'assurance de l'authentification électronique du GC. **Error! Reference source not found. Error! Reference source not found.**.<br>On PEUT indiquer plusieurs valeurs de NA dans les métadonnées du FI, mais une seule valeur est retournée dans une réponse d'authentification. |
| [SAML2 Meta]<br>Section 2.3.2, ligne 371<br><entityID> | Limitée | L'attribut <entityID> DOIT être convenu par l'entité et la FJGC. |
| [SAML2 Meta]<br>Section 2.3.2.1, ligne 443<br><Organization> | Limitée | On RECOMMANDE que le paramètre <Organization> soit présent et comprenne un attribut OrganizationName ou OrganizationDisplayName. |

| SAML2 * | ASI des STAE<br>Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| [SAML2 Meta]<br>Section 2.3.2.2, ligne 476<br><ContactPerson> | Limitée | L'attribut <ContactPerson> est RECOMMANDÉ L'autorisation électronique suggère d'inclure soit EmailAddress ou TelephoneNumber. |
| [SAML2 Meta]<br>Section 2.4.1, ligne 550<br><RoleDescriptor> | Limitée | • On NE DOIT PAS utiliser l'élément de métadonnées <RoleDescriptor>. |
| [SAML2 Meta]<br>Section 2.4.3, ligne 683<br><IDPSSODescriptor><br>y compris<br>Section 2.4.2, ligne 643<br><SSODescriptorType> | Limitée | • La valeur du paramètre WantAuthnRequestsSigned DOIT correspondre à « vrai ».<br>• Exactement deux instances de l'attribut <SingleLogoutService> DOIVENT être présentes (une pour chacune des liaisons : SOAP et HTTP Redirect).<br>• Exactement un attribut <SingleSignOnService> DOIT être présent. |

| SAML2 * | ASI des STAE<br>Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| [SAML2 Meta]<br>Section 2.4.4, ligne 736<br><SPSSODescriptor><br>y compris<br>Section 2.4.2, ligne 643<br><SSODescriptorType> | Limitée | • La valeur du paramètre AuthnRequestsSigned DOIT correspondre à « vrai ».<br>• La valeur du paramètre WantAssertionsSigned DOIT correspondre à « vrai ».<br>• L'attribut <AssertionConsumerService> DOIT être inclus.<br>• Exactement un attribut <AssertionConsumerService> DOIT avoir la liaison établie à urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST.<br>• Exactement un attribut < ManageNameIDService> PEUT être présent pour communiquer le désir de recevoir le message de résiliation NameID des FI. La liaison DOIT être établie à urn:oasis:names:tc:SAML:2.0:bindings:SOAP. |
| [SAML2 Meta]<br>Section 2.4.5, ligne 828<br><AuthnAuthorityDescriptor> | Limitée | On NE DOIT PAS utiliser l'élément <AuthnAuthorityDescriptor>. |
| [SAML2 Meta]<br>Section 2.4.6, ligne 861<br><PDPDescriptor> | Limitée | On NE DOIT PAS utiliser l'élément <PDPDescriptor>. |

| SAML2 * | ASI des STAE<br>Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| [SAML2 Meta]<br>Section 2.5, ligne 938<br><AffiliationDescriptor> | Limitée | On PEUT utiliser l'attribut <AffiliationDescriptor>.<br>• La FJGC peut constituer des groupes d'affiliation des FS de la FJGC qui utiliseront un IAP commun. Dans ce cas, la FJGC fournira des métadonnées définissant ces groupes. |
| [SAML2 MetaUI]<br>Section 2.1.1<br><md:UIInfo> | Prise en charge | Les métadonnées du FS PEUVENT inclure les éléments <mdui:DisplayName> et <mdui:Logo><br>Le FI PEUT utiliser ces éléments de métadonnées pour informer l'utilisateur sur l'entité qui demande une authentification pendant le dialogue sur l'authentification connexe. |
| Fin du tableau | | |

## 2.3 Autres extensions liées aux spécifications [SAML2 *]

En plus des contraintes imposées par ce profil de déploiement sur le profil eGov 2.0 [eGov 2.0] publié par Kantara Initiative, ce document sur les exigences de déploiement de l'authentification électronique élargit également les spécifications sous-jacentes SAML 2.0 publiées par le CTSS d'OASIS.

| SAML2 * | ASI des STAE<br>Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Aucun défini | | |

| SAML2 * | ASI des STAE<br>Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| Fin du tableau | | |

## 2.4 Autres exigences du GC

En plus des contraintes imposées par ce profil de déploiement sur le profil eGov 2.0 [eGov 2.0] publié par Kantara Initiative, des contraintes et des extensions supplémentaires sur les spécifications sous-jacentes SAML 2.0 publiées par le CTSS d'OASIS, ce document sur les exigences de déploiement de l'authentification électronique impose également des exigences supplémentaires pour l'environnement d'authentification électronique du GC.

### 2.4.1 Attributs d'affirmation requis

| Exigence de l'authentification électronique | ASI des STAE<br>Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| [SAML2 Core]<br>Section 2.7.3, ligne 1165<br><AttributeStatement> | Prolongée | Les déploiements de l'authentification électronique du FS et du FI DOIVENT prendre en charge les attributs obligatoires de l'authentification électronique.<br>• Comme indiqué dans la section 2.4.1.1 Attributs obligatoires. |
| [SAML2 Core]<br>Section 2.7.3, ligne 1165<br><AttributeStatement> | Prolongée | Les déploiements de l'authentification électronique du FI PEUVENT prendre en charge les attributs facultatifs de l'authentification électronique.<br>• Comme indiqué dans la section 2.4.1.2 Attributs facultatifs. |

| Exigence de l'authentification électronique | ASI des STAE<br>Prise en charge requise | Renseignements sur le déploiement de l'authentification électronique |
|---|---|---|
| [SAML2 Core]<br>Section 2.7.3, ligne 1165<br><AttributeStatement> | Limitée | Les déploiements du FS de l'authentification électronique NE DEVRAIENT PAS prendre en charge la réception d'autres attributs.<br>• Un déploiement du FS de l'authentification électronique DOIT ignorer tous autres attributs et ne pas utiliser les valeurs d'attribut pour tout traitement. |
| Fin du tableau | | |

#### 2.4.1.1 Attributs obligatoires

| Nom (URL) | Description | Format | Type de données |
|---|---|---|---|
| ca:gc:cyber-authentication:basic:specVer | Version des spécifications de l'interface | DOIT être « 2.0 » pour cette spécification de l'interface [CATS2 IA&S]. | xs:string |
| Fin du tableau | | | |

#### 2.4.1.2 Attributs facultatifs

| Nom (URL) | Description | Format | Type de données |
|---|---|---|---|
| ca:gc:cyber-authentication:basic:assuranceLevel | Déprécié :<br>seulement inclus pour la transition à partir de la version 1 de [CATS1 IA&S]<br>Le niveau de confiance du mécanisme final d'authentification | DOIT correspondre à « 1 », « 2 », « 3 », « 4 » ou « Test ». | xs:string |
| urn:oid: 2.16.840.1.113730.3.1.39 | Déprécié :<br>seulement inclus pour la transition à partir de la version 1 de [CATS1 IA&S]<br>La langue préférée de l'utilisateur final (on s'attend à ce que cette valeur soit définie lorsque l'utilisateur final modifie sa préférence linguistique dans le cadre de ses échanges avec le FI). | DOIT se conformer à la définition du champ de l'en-tête de la langue acceptée (« Accept-Language ») dans [RFC2068], à une réserve près : la séquence « Accept-Language » : « # » devrait être omis. | xs:string |
| Fin du tableau | | | |

### 2.4.2 Niveaux d'assurance de l'authentification électronique du GC

Les demandes et les réponses d'authentification pour les justificatifs d'authentification électronique du GC porteront le niveau d'assurance du GC nécessaire. Il y a quatre niveaux d'assurance qui sont définis dans [ITSG-31] et utilisés par l'Initiative d'authentification électronique du GC. Les URL représentant ces NA du GC ont des valeurs qui sont définies par l'exploitant du FJGC dans [GCCF Values]. Le modèle de ces valeurs est fourni à l'Annexe B : B.1.1 Niveaux d'assurance (NA). Appendix B: **Error! Reference source not found. Error! Reference source not found.** Veuillez prendre note que plusieurs valeurs peuvent être définies pour chaque NA.

### 2.4.3 Communication des préférences linguistiques

Pour répondre aux exigences de la politique du GC, une méthode était nécessaire pour envoyer la préférence linguistique actuelle de l'utilisateur (pas du navigateur) du FS au FI et du FI au FS dans tous les cas, même lorsque l'authentification échoue et qu'une

affirmation n'est pas produite. L'authentification électronique effectuera cela à l'aide d'un témoin de séance dans un domaine commun défini par la FJGC (qui peut être le même domaine établi pour le profil de détection du FI).

Ce témoin de séance portera l'attribut de langue, dont les valeurs sont définies dans la norme [ISO 639-2/T]. Voici les valeurs acceptables pour l'attribut de langue de l'authentification électronique :

- eng
- fra

Les FS et les FI DOIVENT lire ce témoin et utiliser ce paramètre de langue dans toutes pages de l'interface utilisateur qui sont affichées.

Les FS et les FI DOIVENT veiller à ce que ce témoin soit établi à la préférence linguistique actuelle de l'utilisateur avant d'émettre un message sur une liaison HTTP-Redirect ou HTTP-Post. Puisqu'on s'attend à ce que ce témoin de langue du GC soit utilisé, que l'utilisateur soit dans un scénario de demande d'authentification ou de réponse ou non, il devrait être mis à jour le plus tôt possible.

Les renseignements du témoin de langue du GC dans le domaine commun sont fournis dans une annexe du présent document.

### 2.4.4 Protocole de gestion des identificateurs de nom

Un certain nombre de ministères du GC exige un avis en cas de révocation de justificatif. Pour prendre en charge cette capacité, [CATS2 IA&S] ajoute la prise en charge du Protocole de gestion des identificateurs de nom SAML (et le profil).

Les FS formulent leur désir de recevoir ces messages en ajoutant un élément `<ManageNameIDService>` à leur `SPSSODescriptor` dans les métadonnées de FS.

Les FI DOIVENT envoyer un `<ManageNameIDRequest>` pour signaler les FS au cas où un NameID déjà envoyé au FS a été révoqué au FI. Les FI DOIVENT envoyer ces messages de résiliation NameID aux FS pour qui ils ont déjà envoyé des affirmations pour le même principal et NE DEVRAIENT PAS envoyer ces messages de résiliation NameID aux autres FS. Les messages sont envoyés sur le canal arrière et DEVRAIENT être envoyés d'une façon rapide qui est approuvée par la FJGC. Pour prendre en charge ceci, les FI DOIVENT ajouter un élément `<ManageNameIDService>` à leur `IDPSSODescriptor` dans les métadonnées du FI.

Les STAE2 utilisent des IAP qui sont des identificateurs persistants SAML [SAML2 Core, 3,7] et [SAML2 errata, E78]. Cela exige aux FI de tenir à jour « … un identificateur opaque persistant pour un principal... » et « une valeur donnée, une fois associée à un principal, NE DOIT PAS être attribuée à un principal différent à n'importe quel moment dans l'avenir. »

### 2.4.5 Sécurité

Pour établir des liens de confiance et veiller à ce que les communications soient sécurisées, ces spécifications de l'interface s'appuient, dans une très large mesure, sur des paires de clés cryptographiques X.509v3. La présente section décrit les différents certificats qui s'avèrent nécessaires, en plus de fournir de plus amples renseignements sur leur utilisation.

#### 2.4.5.1 Les certificats du Service de GJI du GC

La GJI du GC, exploitée par Services partagés du Canada au nom du GC, fournit de la confiance et de la sécurité à la FJGC. La possession des certificats valides émis par la GJI du GC est requise pour l'interfonctionnement dans la FJGC. La GJI du GC émet deux certificats à chaque FS ou FI (un utilisé pour une signature numérique et un pour le chiffrement).

- Ces certificats DOIVENT être gérés conformément aux responsabilités qui incombent aux abonnés (telles que précisées par la FJGC).

#### 2.4.5.2 Signature numérique

Tous les messages SAML, ou les parties de ceux-ci, DOIVENT être signés par l'expéditeur à l'aide du certificat de signature du Service de GJI du GC qui leur a été délivré. La signature permet au destinataire du message d'authentifier l'expéditeur, en plus de confirmer que le message n'a pas été modifié depuis qu'il a été signé.

- Le destinataire DOIT authentifier l'expéditeur et vérifier la signature sur réception du message.
- Le destinataire DOIT vérifier l'état de révocation du certificat de l'expéditeur ayant servi à signer le message. Les systèmes membres de la Fédération DOIVENT utiliser la méthode suivante pour la vérification de la révocation :
    - LRC – l'emplacement de la liste de révocation des certificats (dans le répertoire ou sur le site Web) peut être imprimé de manière statique dans le logiciel, la liste étant téléchargée périodiquement. Consultez les documents de la GJI du GC (disponible auprès de la FJGC) pour les détails concernant l'emplacement de nom distingué et du nom d'hôte du répertoire.
- S'il s'avère impossible de déterminer l'état de la révocation du certificat, le système membre du regroupement DOIT rejeter le message.

#### 2.4.5.3 Chiffrement

Le chiffrement permet de veiller à ce que seul le destinataire souhaité puisse déchiffrer le message et accéder à l'information confidentielle qui s'y trouve.

- Toute l'information confidentielle qui est intégrée à un message SAML DOIT être chiffrée.

- Le chiffrement DOIT avoir recours à la clé publique du certificat de chiffrement délivré par la GJI du GC du destinataire prévu.

#### 2.4.5.4 Sites Web TLS

##### 2.4.5.4.1 Pour les liaisons du canal avant

Cette spécification de l'interface indique les liaisons du canal avant utilisant le protocole HTTP sur TLS (HTTPS) pour acheminer des messages.

- Tout site géré par un membre de la Fédération et utilisant des liaisons HTTP sur TLS DOIT sécuriser la séance TLS à l'aide d'un certificat de confiance par défaut par les navigateurs disponibles sur le marché.
- L'utilisation du protocole TLS DOIT être conforme aux directives du CST ([ITSP.40.062]) et aux politiques du ministère.
- On DOIT utiliser le protocole HTTPS sur TLS (v1.1 ou version plus) à moins que le navigateur ne le prenne pas en charge.
- Le protocole HTTPS sur TLS (v1.0) peut être utilisé.
- Les versions antérieures du protocole TLS ou SSL NE DOIVENT pas être utilisées.

##### 2.4.5.4.2 Pour les liaisons du canal arrière

Cette spécification de l'interface indique les liaisons du canal arrière à l'aide du protocole SOAP sur TLS pour acheminer des messages.

- Tout site géré par un membre de la Fédération et utilisant des liaisons SOAP sur TLS DOIT sécuriser la séance TLS à l'aide d'un certificat de confiance par défaut par les navigateurs disponibles sur le marché.
- L'utilisation du protocole TLS DOIT être conforme aux directives du CST ([ITSP.40.062]) et aux politiques du ministère.
- Le protocole TLS (v1.1 ou ultérieure) DOIT être utilisé.
- Les versions antérieures du protocole TLS ou SSL NE DOIVENT pas être utilisées.

### 2.4.6 Traitement des exceptions

| Prise en charge obligatoire de l'interface de l'authentification électronique | Renseignements sur le déploiement de l'authentification électronique |
|---|---|
| Le service SAML des membres de l'authentification électronique DOIVENT traiter les conditions d'erreur gracieusement. | Plus précisément, le service SAML des membres de l'authentification électronique DOIT traiter la liste des erreurs possibles fournie à la section 2.4.6.1 Erreurs à traiter. |

#### 2.4.6.1 Erreurs à traiter

Le tableau suivant énumère les erreurs que le service SAML des membres de la Fédération DOIT traiter gracieusement (c'est-à-dire, d'une manière conviviale et contrôlée selon la capacité de réponse du FI ou du FS). Le tableau répertorie les erreurs par événement SAML.

| Condition d'erreur |
| --- |
| Erreur de traitement <Response><br>• <Issuer> incorrect/inconnu<br>• Version erronée<br>• Valeur non reconnue du paramètre InResponseTo<br>• Valeur non acceptable du paramètre IssueInstant<br>• État : Échec |
| Erreur de traitement <Assertion><br>• Signature invalide<br>• Certificat de signature révoqué<br>• Impossible d'établir l'état de la révocation<br>• Temps de l'élément <Assertion> non valide<br>• Impossible de déchiffrer l'élément <Assertion><br>• Destinataire erroné<br>• Version erronée |
| Erreur de traitement <AuthnRequest><br>• <Issuer> inconnu<br>• Signature invalide<br>• Certificat de signature révoqué<br>• Impossible d'établir l'état de la révocation |

| |
|---|
| Traitement des erreurs – Demande de SLO<br>• <Issuer> inconnu<br>• Signature invalide<br>• Certificat de signature révoqué<br>• Impossible d'établir l'état de la révocation |
| Traitement des erreurs SLO <Response><br>• <Issuer> inconnu<br>• Signature invalide<br>• État inconnu<br>• Certificat de signature révoqué<br>• Impossible d'établir l'état de la révocation |

# Appendix A: Fonctions supplémentaires au-delà de l'authentification électronique (normative)

## A.1. Témoin de langue du GC

Cette annexe définit une méthode par laquelle un FS ou un FI peut détecter la langue que le principal utilise actuellement. Cette méthode repose sur un témoin qui est rédigé dans un domaine qui est commun entre les FI et les FS dans le déploiement de la FJGC. Ce domaine est établi par la FJGC et peut être le même que le domaine commun utilisé pour le profil de détection du FI et est appelé `<common-domain>` dans ce profil, et le témoin contenant la dernière langue d'utilisation est appelé témoin de langue du GC.

Dans la FJGC, les entités du FS et du FI doivent héberger des serveurs Web dans le domaine commun comme indiqué par la FJGC.

### A.1.1 Le témoin de langue du GC est dans un domaine commun du GC

Le nom du témoin DOIT être « _gc_lang ». Le format de la valeur du témoin DOIT être une seule chaîne de texte valorisée.

Le service de rédaction des témoins du domaine commun (voir ci-dessous) DEVRAIT mettre à jour la valeur de langue lorsque l'utilisateur indique une autre langue préférée. L'objectif est que la langue la plus récemment établie est celle dans le témoin. Les valeurs du témoin de langue du GC sont définies dans la norme [ISO 639-2/T]. Voici les valeurs acceptables pour le témoin de langue du GC :

- eng
- fra

Le témoin DOIT être établi avec un préfixe de chemin de « / ». Le domaine DOIT être réglé à « .<common-gc-domain> où <common-gc-domain> est le domaine commun du GC établi par la FJGC pour être utilisé avec cette méthode (on peut également l'utiliser avec le profil de détection du FI). Il DOIT y avoir une période principale. Le témoin DOIT être marqué comme sécurisé.

La syntaxe du témoin devrait être conforme avec la norme RFC 2965 d'Internet Engineering Task Force (IETF). Le témoin DOIT être pour la séance uniquement.

### A.1.2 Obtention du témoin de langue du GC

Avant de présenter un dialogue d'authentification au principal, un FI DOIT connaître la langue de communication préférée du principal. Pour ce faire, le FI DOIT faire appel à un échange conçu pour présenter le témoin de langue du GC au FI après qu'il soit lu par un serveur HTTP dans le domaine commun.

Les moyens précis par lesquels le FS lit le témoin sont propres à la mise en œuvre tant qu'elle est en mesure de pousser l'agent utilisateur à présenter des témoins qui ont été établis avec les paramètres appropriés. Une stratégie de mise en œuvre possible est décrite comme suit et devrait être considérée comme non normative. De plus, elle peut être sous-optimale pour certaines applications.

- Avoir déjà établi un DNS et un alias d'IP pour elle-même dans le domaine commun.
- Réorienter l'agent utilisateur à elle-même en utilisant l'alias de DNS à l'aide d'une URL indiquant « http » comme le modèle d'URL. La structure de l'URL est privée à la mise en œuvre et peut inclure des renseignements de séance nécessaires pour identifier l'agent utilisateur.
- Réorienter l'agent utilisateur de retour à elle-même.

### A.1.3 Établissement du témoin de langue du GC

- Avant d'invoquer une demande d'authentification, un FS DOIT veiller à ce que le témoin de langue du GC soit réglé à la langue préférée du principal. Avant d'envoyer une réponse d'authentification (y compris les réponses d'erreur), un FI DOIT veiller à ce que la langue de témoin du GC soit établie à la langue préférée du principal. À un moment donné que le principal décide de changer sa langue, le FS ou le FI PEUT établir le témoin de langue du GC. Les moyens par lesquels le FS ou le FI établit le témoin sont propres à la mise en œuvre tant que le témoin est bien établi avec les paramètres ci-dessus. Une stratégie de mise en œuvre possible est décrite comme suit et devrait être considérée comme. Le FS ou le FI peut :
- Avoir déjà établi un alias de DNS et d'IP non normative pour elle-même dans le domaine commun.
- Réorienter l'agent utilisateur à elle-même en utilisant l'alias de DNS à l'aide d'une URL indiquant « http » comme le modèle d'URL. La structure de l'URL est privée à la mise en œuvre et peut inclure des renseignements de séance nécessaires pour identifier l'agent utilisateur.
- Établir le témoin sur l'agent utilisateur réorienté à l'aide des paramètres indiqués ci-dessus.
- Réorienter l'agent utilisateur de retour à elle-même.

# Appendix B: Exigences opérationnelles de la FJGC (Normatives)

## B.1. Modèle des valeurs opérationnelles de la FJGC

Les valeurs opérationnelles suivantes de la FJGC sont indiquées dans le document [GCCF Values], qui est fourni par l'opérateur de la FJGC.

### B.1.1 Niveaux d'assurance (NA)

Le paramètre <RequestedAuthnContext> DOIT comprendre un niveau d'assurance comme indiqué dans [SAML2 Assur]. La valeur de NA s'affichera également dans le message <Response> dans <AuthnContext>.

De même, les métadonnées des FI de l'authentification électronique DOIVENT indiquer les NA pris en charge dans l'attribut <assurance-certification> comme indiqué dans [SAML2 Assur], Section 3 Profil des attributs de certification d'assurance de l'identité

Les NA de l'authentification électronique du GC sont définis par l'opérateur de la FJGC. Ils doivent comprendre des valeurs pour chaque NA de NA1 à NA4. Les valeurs doivent être uniques et stables. Il peut y avoir plusieurs valeurs pour chaque NA (p. ex., pour répondre aux exigences linguistiques).

### B.1.2 Paramètre SPNameQualifier

L'opérateur de la FJGC peut constituer des groupes d'affiliation des FS de la FJGC qui utiliseront un IAP commun. Dans ce cas, les FS peuvent utiliser le paramètre <SPNameQualifier> dans la demande d'authentification pour indiquer leur désir pour cet IAP commun. L'opérateur de la FJGC ajoutera également ces groupes d'affiliation aux métadonnées.

### B.1.3 Paramètre SessionNotOnOrAfter

Les déploiements du FI de l'authentification électronique NE DEVRAIENT PAS indiquer l'attribut SessionNotOnOrAfter. Cela permet au FS de choisir sa propre durée requise pour son contexte de sécurité.

Si un FI de la FJGC est incapable de configurer cette valeur pour ne pas être envoyé, il DOIT établir cette valeur à une valeur élevée, comme déterminé par la FJGC.

### B.1.4 Nom de domaine commun

Il y a deux exigences du domaine commun dans ce document des STAE2 qui doivent être abordées par l'opérateur de la FJGC :

- Section 2.1, eGov 2.5.1 Détection du fournisseur d'identité
    - Les déploiements du FI de l'authentification électronique DOIVENT prendre en charge la détection du fournisseur d'identité indiquée dans [SAML2 Prof].
    - Les déploiements du FS de l'authentification électronique PEUVENT prendre en charge la détection du fournisseur d'identité indiquée dans [SAML2 Prof].
- Annexe A.1 Témoin de langue du GC

- « Ce domaine (témoin de langue du GC) est établi par la FJGC et peut être le même que le domaine commun utilisé pour le profil de détection du FI ».