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

Better government: with partners, for Canadians

Solutions technologiques d'authentification électronique

Architecture et spécifications de l'interface

Version 2.0 :

Profil de mise en place

État: Version de base pour la DP n° 3
Version définitive 7.2
Date de modification: le 25 mars, 2011 13:57
Nom du fichier: CA - CATS IA&S V2 0_Deployment Profile_Final r7.2_fr.doc

Pour obtenir de plus amples renseignements, veuillez communiquer avec:
Bob Sunday
Programme d'authentification électronique
Direction du dirigeant principal de l'information
Secrétariat du Conseil du Trésor
613-941-4764
Courriel : robert.sunday@tbs-sct.gc.ca

Approbation par : SCT, CDPI

Comité des DG sur l'authentification électronique

Canada

Fiche des révisions

N° de VERSION	DESCRIPTION	DATE DE DISTRIBUTION	État	AUTORISATION ET NOTES
0.1	Texte initial	17 septembre 2010	Première version – travail en cours	Bob Sunday, SCT
0.2	Version préliminaire à examiner en vue d'une approbation durant l'atelier de l'équipe corsaire de la DP nº 3 (28 octobre)	4 octobre 2010	Version préliminaire définitive	Bob Sunday, SCT
version 4	Document recommandé en vue d'une approbation par les responsables de la gouvernance à titre de document de base	15 novembre 2010	Version de base recommandée	Bob Sunday, SCT Avec beaucoup d'aide des membres de l'équipe d'élite de la DP no 3 et de leurs collègues
version 5	Document de base recommandé pour approbation par le Comité des DG sur l'authentification électronique	19 novembre 2010	Version de base recommandée	Bob Sunday, SCT
version 6 (finale)	Document de base définitif à joindre à l'ébauche de DP n° 3	25 novembre 2010	Version de base pour la DP n° 3	Bob Sunday, SCT
version 7 (finale)	Document de base définitif à joindre à l'ébauche de DP n° 3	14 decembre 2010	Version de base pour la DP n° 3	Bob Sunday, SCT
Ébauche r7.1	Document de base (avec mises à jour proposées) à joindre à la DP n° 3 finale	9 février 2011	Version de base pour la DP n° 3	Bob Sunday, SCT
version 7.2 (finale)	Document de base à joindre à la DP n° 3 finale	25 mars 2011	Version de base pour la DP n° 3	Bob Sunday, SCT

Avant-propos

Note concernant la présente version – ébauche r7.2

Le présent document, « *Solutions technologiques d'authentification électronique – Architecture et spécifications de l'interface – Version 2.0 : Profil de mise en place* » constitue la version de base actualisée du document « *Architecture et spécifications de l'interface de la Solution tactique d'authentification électronique (STAE)* ». La présente version constitue le document de base officiel approuvé par le Comité des DG sur l'authentification électronique en vue d'une distribution avec la DP n° 3.

Les changements apportés par la suite au présent document de base seront traités en même temps que les clauses et demandes officielles de changement.

Table des matières

1 INTRODUCTION 5

1.1 Programme d'authentification électronique – Vision 5

1.2 Vue d'ensemble du Profil de mise en place de l'ASI des STAE 6

1.3 Conformité avec le Profil de mise en place de l'ASI des STAE 7
1.3.1 Notation 8

1.4 Changements par rapport à l'*Architecture de l'interface et spécification de la STAE1* 8
1.4.1 Priorité à la mise en place plutôt qu'à la technologie sous-jacente 9
1.4.2 Prise en charge explicite du niveau d'assurance exigée 9
1.4.3 Envoi OBLIGATOIRE des réponses d'authentification 10
1.4.4 Mise en œuvre OBLIGATOIRE du profil de dépistage des fournisseurs de services de justificatifs d'identité 10
1.4.5 Utilisation des demandes de canal d'appui pour la fermeture de session unique 10
1.4.6 Utilisation du témoin (cookie) de langue du gouvernement pour communiquer la langue 11
1.4.7 Avis de révocation d'un justificatif d'identité 11
1.4.8 Corrections et mises à jour diverses 12

1.5 Documents de référence 12

2 EXIGENCES (NORMATIVES) DE LA MISE EN PLACE 14

2.1 Contraintes pour le Profil eGov 2.0 de l'initiative Kantara 14

2.2 Autres contraintes visant les spécifications [SAML2*] 43

2.3 Autres extensions liées à la spécification [SAML2 *] 49

2.4 Autres exigences du gouvernement 50
2.4.1 Attributs d'assertion requis 50
2.4.2 Niveaux d'assurance de l'authentification électronique du gouvernement 53
2.4.3 Communication des préférences linguistiques 53
2.4.4 Protocole de gestion d'identificateur de nom 54
2.4.5 Sécurité 54
2.4.6 Traitement des exceptions 56

ANNEXE A: AUTRES FONCTIONS EN PLUS DE L'AUTHENTIFICATION ÉLECTRONIQUE (NORMATIVES) 60

A.1. Témoin de langue du GC 60
A.1.1 Témoin de langue du GC stocké dans un domaine commun du GC 60
A.1.2 Obtention du témoin de langue du GC 60
A.1.3 Définition du témoin de langue du GC 61

1 Introduction

1.1 Programme d'authentification électronique – Vision

La vision du Programme d'authentification électronique du gouvernement du Canada est partiellement illustrée ci-dessous.

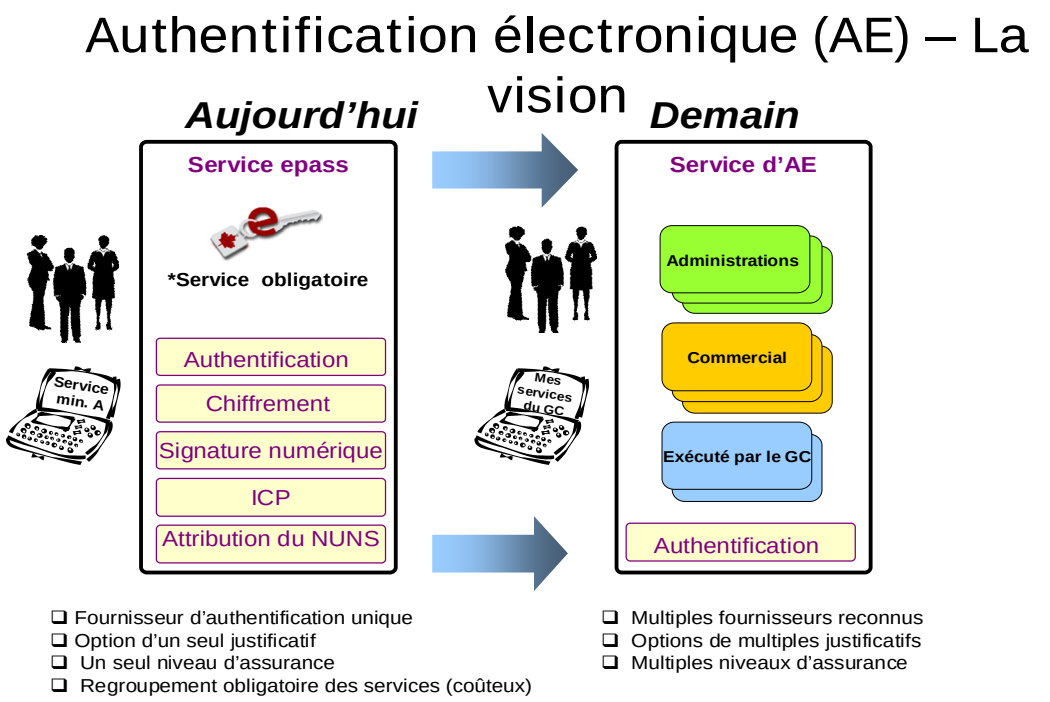

Figure 1 : Vision de l'authentification électronique

1.2 Vue d'ensemble du Profil de mise en place de l'ASI des STAE

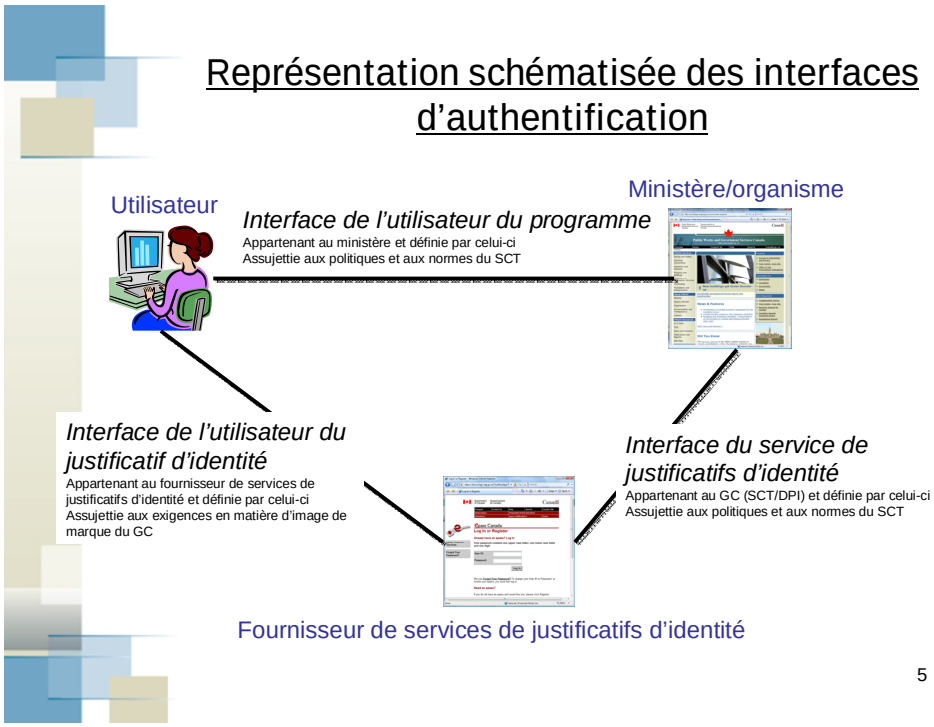

Figure 2 : Représentation schématisée des interfaces d'authentification

Le présent « *Profil de mise en place de l'ASI des STAE* » [ASI STAE 2] est un profil de mise en place qui vise une participation à l'environnement d'authentification électronique du gouvernement du Canada. Il décrit l'interface de messagerie « Interface du service de justificatifs d'identité » qui est précisée à la figure 2, Représentation schématisée des interfaces d'authentification.

Il porte sur les services configurés pour participer à titre de fournisseurs de services et de fournisseurs de services de justificatifs d'identité (FSJ). Au sein du gouvernement du Canada, les fournisseurs de services sont également appelés parties utilisatrices (PU) (il s'agit en général de services ministériels en ligne), tandis que les fournisseurs d'identificateurs sont appelés fournisseurs de services de justificatifs d'identité (FSJ). Le GC utilise également le terme courtier de justificatifs d'identité (CJI), qui est une entité de système qui agit à la fois comme fournisseur de services de justificatifs d'identité pour les PU et en tant que PU lorsqu'il communique avec les fournisseurs de services de justificatifs d'identité connexes. Dans ces situations, la documentation du SAML utilise le terme Mise en cache du fournisseur de services de justificatifs d'identité.

NOTA : Dans le présent document, nous employons les termes « fournisseurs de services » et « fournisseurs de services de justificatifs d'identité ». D'autres documents sur l'authentification électronique emploient également les termes parties utilisatrices et fournisseurs de services de justificatifs d'identité. La documentation du SAML (langage de balisage des déclarations de sécurité) et de l'initiative Kantara utilise les termes « fournisseurs de services » et « fournisseurs d'identificateurs ». Nous n'utilisons pas le terme courtier de justificatifs d'identité (CJI) dans le présent document, du fait qu'il s'agit d'une combinaison des rôles de fournisseur de services et de fournisseur de services de justificatifs d'identité.

Le Profil de mise en place est une version peaufinée de l'ancien document du gouvernement « *Architecture de l'interface et spécification de la solution tactique d'authentification électronique (STAE)* » [ASI STAE 1]

Ce profil n'est pas un tutoriel ni un document d'orientation. L'OGFJGC pourra proposer d'autres directives et des cas d'utilisation.

1.3 Conformité avec le Profil de mise en place de l'ASI des STAE

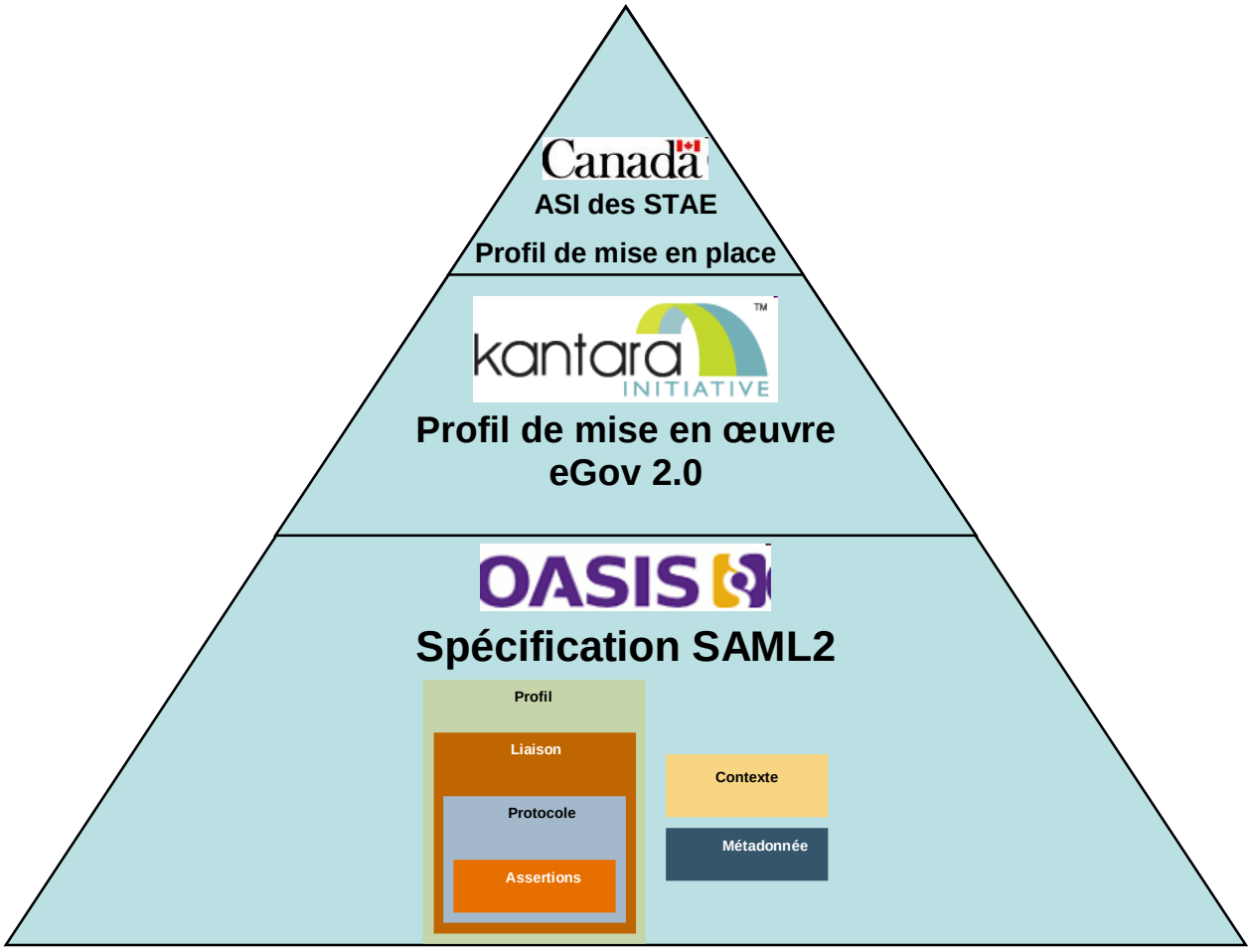

Figure 3 : Modules de l'architecture de l'interface de l'authentification électronique

Le Profil de mise en place est fondé sur le Profil eGov 2.0 [eGov 2.0] publié par l'initiative Kantara, sans toutefois lui être parfaitement conforme. Les exigences normatives du présent Profil de mise en place du gouvernement qui touchent les sections pertinentes du Profil eGov 2.0 sont décrites à la section 2 du présent document. Le Profil eGov 2.0 se fonde sur les spécifications SAML 2.0 élaborées par le Security Services Technical Committee (SSTC) d'OASIS, mais restreint les caractéristiques, éléments, attributs et autres valeurs de base de SAML 2.0 exigées pour les fédérations et les mises en place du gouvernement électronique. Les actions et les caractéristiques SAML respectent celles des spécifications OASIS SAML 2.0 [SAML2*], sauf indication contraire.

NOTA : Les essais d'interopérabilité réalisés par des organismes externes, comme l'initiative Kantara, peuvent aider à vérifier la conformité. Ainsi, les acquisitions du gouvernement qui doivent être conformes au présent Profil de mise en place peuvent également exiger que les logiciels sous-jacents respectent les essais d'interopérabilité extérieurs.

Toutefois, ces essais extérieurs ne constituent pas une vérification complète et définitive de la conformité avec les exigences de mise en place du gouvernement. D'autres essais peuvent ainsi être exigés par l'Organe de gouvernance de la fédération des justificatifs du GC (OGFJGC) en vue d'une participation à la FJGC.

1.3.1 Notation

Cette spécification utilise du texte normatif pour décrire les capacités en SAML.

Dans ce contexte, il faut interpréter les mots clés « MUST », « MUST NOT », « REQUIRED », « SHALL », « SHALL NOT », « SHOULD », « SHOULD NOT », « RECOMMENDED » « MAY » et « OPTIONAL » de la manière décrite dans le document [RFC2119] :

> …il FAUT les utiliser seulement lorsqu'ils sont nécessaires à des fins d'interopérabilité ou pour limiter les opérations qui risquent du causer du tort (p. ex., en limitant les retransmissions)…

Ces mots clés sont donc écrits en majuscules lorsqu'ils doivent servir à spécifier de façon non ambiguë des exigences au-delà des protocoles et touchant des fonctions des applications et opérations qui affectent l'interopérabilité et la sécurité des applications.

1.4 Changements par rapport à l'*Architecture de l'interface et spécification de la STAE1*

Le présent document diffère du document [ASI STAE 1] à plusieurs égards :

1.4.1 Priorité à la mise en place plutôt qu'à la technologie sous-jacente
1.4.2 Prise en charge explicite du niveau d'assurance exigée
1.4.3 Envoi OBLIGATOIRE des réponses d'authentification
1.4.4 Mise en œuvre OBLIGATOIRE du profil de dépistage des fournisseurs de services de justificatifs d'identité
1.4.5 Utilisation des demandes de canal d'appui pour la fermeture de session unique

1.4.6 Utilisation du témoin (cookie) de langue du gouvernement pour communiquer la langue
1.4.7 Avis de révocation d'un justificatif d'identité
1.4.8 Corrections et mises à jour diverses

Ces changements sont décrits de façon générale ci-après. Pour connaître tous les détails de la conformité normative imposée au présent Profil de mise en place, reportez-vous à la section 2 du présent document, « Exigences (normatives) de la mise en place ».

1.4.1 Priorité à la mise en place plutôt qu'à la technologie sous-jacente

Le présent document du Profil de mise en place assouplit les règles, mais pas les exigences liées à la conformité, qui stipulaient auparavant que les logiciels sous-jacents des fournisseurs de services et des fournisseurs de services de justificatifs d'identité réussissent les essais d'interopérabilité.

Les nouvelles règles vont exiger la mise en place du « service » du fournisseur de services de justificatifs d'identité et du fournisseur de services en vue des essais d'interopérabilité et d'une certification en fonction des règles précisées dans le présent document de Profil de mise en place.

Les documents du plan d'essai de l'initiative Kantara indiquent de nombreux jeux d'essais avec lesquels on peut vérifier de nombreuses sections du présent Profil de mise en place; ils aideront grandement la FJGC à établir la conformité. En outre, le fait d'utiliser des logiciels commerciaux ayant réussi les essais d'interopérabilité de la Liberty Alliance ou de l'initiative Kantara augmente beaucoup les chances de respecter adéquatement les exigences de mise en place établies.

Il découle de cette réorientation que l'Organe de gouvernance de la fédération des justificatifs du GC (OGFJGC) devient l'organisme autorisé à déterminer si une mise en place (fournisseur de services ou fournisseur de services de justificatifs d'identité) a fait l'objet d'essais suffisants pour que le service en question fasse partie de la fédération.

1.4.2 Prise en charge explicite du niveau d'assurance exigée

Le FJGC appuie plusieurs niveaux d'assurance et, ainsi, on doit préciser le niveau souhaité (pour le fournisseur de services) et le niveau fourni (par le fournisseur de services de justificatifs d'identité). Le soutien du niveau d'assurance est exigé conformément au document [SAML2 Assurance]. Les niveaux d'assurances d'authentification électronique du gouvernement du Canada sont décrits dans le document [ITSG-31] et les URI correspondants sont précisés dans le présent « *Profil de mise en place de l'ASI des STAE* », à la section 2.4.2, Niveaux d'assurance de l'authentification électronique du gouvernement du Canada.

Les fournisseurs de services doivent demander un niveau d'assurance du gouvernement du Canada précis avec l'opérateur de comparaison « exact ». Précisons que le fournisseur peut indiquer que plus d'un niveau d'assurance est acceptable. Une situation de la sorte peut s'avérer utile dans les cas où le niveau 2 est requis, mais si le fournisseur de services est disposé à accepter (et peut-être à payer les frais correspondants) au niveau 3 si le niveau 2 n'est pas réalisable.

Il faut configurer les fournisseurs de services de justificatifs d'identité pour les faire correspondre au(x) niveau(x) d'assurance exact(s) pour lesquels ils sont certifiés. Les fournisseurs de services de justificatifs d'identité doivent rejeter toute demande d'authentification d'un niveau d'assurance pour lequel ils n'ont pas été certifiés en précisant le codé d'état approprié. Les fournisseurs de services de justificatifs d'identité doivent fournir le niveau d'assurance précis demandé.

Les exigences visant les métadonnées portent notamment sur la prise en charge additionnelle du niveau d'assurance, conformément aux détails du document [SAML2 Assurance].

1.4.3 Envoi OBLIGATOIRE des réponses d'authentification

Les produits commerciaux existants diffèrent sur le plan de la capacité à envoyer des réponses d'authentification dans certains cas, pendant le traitement de la demande d'authentification. Dans le STAE1, l'utilisateur se butait alors à un problème (par exemple, l'utilisateur pouvait annuler l'ouverture de session).

Le Profil eGov 2.0 [eGov 2.0] de l'initiative Kantara exige désormais qu'on produise et envoie les réponses, que la demande d'authentification réussisse ou non. Cette exigence est également précisée par le présent « *Profil de mise en place de l'ASI des STAE* », et elle favorisera l'amélioration de la messagerie utilisateur et une meilleure continuité du dialogue des utilisateurs.

1.4.4 Mise en œuvre OBLIGATOIRE du profil de dépistage des fournisseurs de services de justificatifs d'identité

Dans un environnement à un seul fournisseur de services de justificatifs d'identité, il n'était pas nécessaire d'indiquer le fournisseur auquel l'utilisateur souhaitait faire appel. Ainsi, l'exigence de la STAE1 pour le profil de dépistage, qui permet à l'utilisateur de choisir son fournisseur de services de justificatifs d'identité, a été reportée pour les fournisseurs de services et les fournisseurs de services de justificatifs d'identité.

L'environnement du gouvernement du Canada, qui appuie désormais plusieurs fournisseurs de services de justificatifs d'identité, exige donc un mécanisme de prise en charge du choix du fournisseur de services par l'utilisateur et le fournisseur de services de justificatifs d'identité.

Le présent « *Profil de mise en place de l'ASI des STAE* » ne modifie pas la spécification du document [ASI STAE 1], mais il exige désormais l'inclusion dans la mise en place du profil de dépistage du fournisseur de services de justificatifs d'identité. Il se peut donc que les fournisseurs de services et les fournisseurs de services de justificatifs d'identité existants doivent modifier leurs services en conséquence.

1.4.5 Utilisation des demandes de canal d'appui pour la fermeture de session unique

Les installations existantes appuient la fermeture de session unique à l'aide des liaisons de canal d'avant-plan SAML, qui font communiquer le navigateur de l'utilisateur tour à tour avec chaque fournisseur de services. En d'autres termes, les fermetures de session de chaque fournisseur de services sont effectuées successivement, ce qui augmente les risques qu'une erreur laisse l'utilisateur dans un état indéterminé.

Pour améliorer cette situation, la STAE2 ajoute l'appui des liaisons de canal d'appui, afin de prendre en charge la fermeture de session unique, et elle empêche la propagation des fermetures de session en avant-plan vers les autres PU touchées. Les liaisons SOAP sont ainsi prises en charge pour les demandes et les réponses de fermeture de session, conformément aux spécifications du Profil eGov 2.0 [eGov 2.0].

Le ministère peut donc maintenant :

- garder le contrôle de la session de l'utilisateur et indiquer au fournisseur de services de justificatifs d'identité de fermer la session; ou
- laisser au fournisseur de services de justificatifs d'identité le contrôle de la session de l'utilisateur,
    - afin de permettre au fournisseur de services de justificatifs d'identité d'informer l'utilisateur au sujet d'erreurs précises pouvant survenir et, à la fin de la session, de rediriger l'utilisateur au fournisseur de services.

1.4.6 Utilisation du témoin (cookie) de langue du gouvernement pour communiquer la langue

La *Loi sur les langues officielles* (LLO) du gouvernement du Canada et la Politique sur la Normalisation des sites Internet stipulent l'utilisation systématique d'un moyen de communication de la préférence de langue de l'utilisateur, même si l'authentification échoue et qu'aucune assertion n'est produite.

La STAE1 n'a prévu aucun mécanisme de transmission au fournisseur de services de la langue de l'utilisateur. La clé d'accès du gouvernement devait ainsi présenter une première page bilingue et il était alors impossible de communiquer un changement de langue en cas d'échec de l'authentification, ce qui n'était pas entièrement conforme aux exigences de la LLO.

La STAE2 prévoit plutôt pour l'authentification électronique l'utilisation d'un témoin de langue du gouvernement. Ce témoin lié à la session est mis à jour et lu par les fournisseurs de services et les fournisseurs de services de justificatifs d'identité s'il leur faut connaître la langue de l'utilisateur, afin de respecter les exigences de la LLO.

Nota : Bien que cette fonction soit nécessaire pour l'authentification électronique, son utilisation s'applique aussi à d'autres situations propres au gouvernement, comme les portails. Afin qu'elle puisse être adjointe à une norme gouvernementale future plus pertinente, elle a été définie de façon générique et présentée dans une annexe du présent document.

1.4.7 Avis de révocation d'un justificatif d'identité

La STAE1 ne prévoyait aucun mécanisme d'avis à un ministère si un fournisseur de services de justificatifs d'identité annulait un justificatif d'identité utilisé au sein de ce ministère. Or, plusieurs ministères ont besoin d'une telle fonction afin de mieux gérer leurs effectifs.

La STAE2 prévoit la prise en charge par les fournisseurs de services de justificatifs d'identité de l'envoi de ces données par demandes de canal d'appui, à l'aide du protocole, et du profil, de gestion d'identificateurs de nom SAML.

Ces améliorations permettent aux fournisseurs de services d'indiquer à l'aide de métadonnées qu'ils souhaitent recevoir ces messages, et le GC peut aussi exiger des fournisseurs de services de justificatifs d'identité qu'ils avisent un fournisseur de services en cas d'annulation d'un justificatif d'identité utilisé auparavant par ce fournisseur de services. Les fournisseurs de services de justificatifs d'identité ne doivent informer un fournisseur de services de l'annulation d'un code d'utilisateur que s'ils ont déjà transmis des assertions à ce fournisseur pour l'utilisateur visé.

1.4.8 Corrections et mises à jour diverses

Différentes corrections et mises à jour doivent être effectuées :

- Afin de traiter correctement les IAP envoyés à plusieurs ministères, l'identificateur de nom (`<NameID>`) qui figure dans l'assertion peut comprendre le qualificatif de nom du fournisseur de service (`SPNameQualifier`), ce qui corrige un bogue de la STAE1.
- Toutes les fermetures de session sont globales. Ainsi, toute fermeture entraîne la transmission d'un profil complet de fermeture de session unique à tous les fournisseurs de services qui prennent part à la session de l'utilisateur. Le fournisseur de services de justificatifs d'identité ou le fournisseur de services n'aura plus à demander le choix entre une fermeture de session locale et une fermeture globale, ce qui règle un problème de convivialité.
- L'indication `RelayState` ne doit pas être transmise dans les messages de réponse d'authentification, sauf si elle a été reçue dans le message correspondant de demande d'authentification. Cela règle un bogue de la STAE1.
- L'indication `SessionNotOnOrAfter` ne doit pas être transmise dans les messages de réponse d'authentification électronique, ce qui permet au fournisseur de services d'établir lui-même le délai de temporisation. Cela règle un problème de convivialité.
- La signature graphique du fournisseur de services et le nom à afficher sont ajoutés aux métadonnées du fournisseur de services. La STAE2 peut ainsi respecter d'éventuelles exigences en matière d'association de marques.

1.5 Documents de référence

[ASI STAE 1]	« Architecture de l'interface et spécification de la Solution tactique d'authentification électronique (STAE) Version 1.0 », 23 janvier 2009.
[ASI STAE 2]	« Solutions technologiques d'authentification électronique – Architecture et spécifications de l'interface – Version 2.0 : Profil de mise en place »; le présent document.
[eGov 2.0]	« Kantara Initiative eGovernment Implementation Profile of SAML V2.0 » (initiative Kantara, version 2.0 du profil de mise en œuvre du gouvernement électronique SAML 2.0) : http://kantarainitiative.org/confluence/download/attachments/42139782/kantara-egov-saml2-profile-2.0.pdf
[ITSG-31]	« Conseils en matière de sécurité des TI (ITSG), Guide sur l'authentification des utilisateurs pour les systèmes TI », publié par le

Centre de la sécurité des télécommunications Canada; consultable à l'adresse suivante : http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/index-fra.html

[RFC 1766] Tags for the Identification of Languages (Balises pour la désignation des langues) http://www.ietf.org/rfc/rfc1766.txt

[RFC2119] Key words for use in RFCs to Indicate Requirement Levels (Mots clés à utiliser dans les documents pour indiquer les niveaux d'exigences) http://www.ietf.org/rfc/rfc2119.txt

[SAML2 *] Tous les documents de référence SAML2 sont offerts à l'adresse suivante : http://docs.oasis-open.org/security/saml/v2.0 ainsi qu'à cette adresse : http://wiki.oasis-open.org/security/FrontPage

[SAML2 Assurance] OASIS Committee Specification 01, SAML V2.0 Identity Assurance Profiles Version 1.0, novembre 2010. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cs-01.pdf [SAML2 Liaisons] OASIS Standard, Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, mars 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

[SAML2 Base] OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, mars 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SAML2 Errata] OASIS SAML V2.0 Approved Errata, 1 decembre 2009. http://www.oasis-open.org/committees/download.php/37166/sstc-saml-approved-errata-2.0-02.pdf

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

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

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

2 Exigences (normatives) de la mise en place

2.1 Contraintes pour le Profil eGov 2.0 de l'initiative Kantara

Cette spécification s'articule autour de l'ensemble de spécifications SAML 2.0 [SAML2 *] et du profil SAML2 appelé « Kantara Initiative eGovernment Implementation Profile of SAML version 2.0 » [eGov 2.0].

Ce Profil de mise en place se fonde sur le Profil eGov 2.0 [eGov 2.0] publié par la Kantara Initiative, sans lui être parfaitement conforme, car cela n'est pas nécessaire (voir la note de la section 1.3, page 7). Bien que le Profil eGov 2.0 de Kantara soit un profil de « mise en œuvre » pour les fournisseurs de logiciels, le présent profil d'authentification électronique est un profil de « mise en place » qui restreint davantage et explique la mise en place des fournisseurs de services et des fournisseurs de services de justificatifs d'identité dans l'environnement d'authentification électronique du gouvernement du Canada. Dans les cas où le « *Profil de mise en place de l'ASI des STAE2* » n'offre pas explicitement d'orientation SAML2, la mise en œuvre doit se conformer aux exigences correspondantes SAML 2.0 d'OASIS.

Le tableau ci-dessous est établi selon l'ordre et la description des exigences des sections 2 et 3 du document [eGov 2.0], répétées telles quelles dans la première colonne. Le tableau indique le soutien requis de la part du Programme d'authentification électronique du gouvernement : en général, il s'agit d'un « prise en charge » ou d'une « contrainte » ou de l'indication « S.O. » (sans objet). Si d'autres détails s'avèrent nécessaires pour expliquer complètement l'exigence du gouvernement, ceux-ci sont présentés dans la troisième colonne.

En outre, des exigences supplémentaires, en plus des exigences eGov 2.0, sont précisées dans les sections qui suivent. L'authentification électronique impose également des contraintes aux spécifications SAML 2.0 et elle comporte peu d'exigences propres à l'authentification électronique.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
eGov 2.2 Metadata and Trust Management		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Identity Provider, Service Provider, and Discovery Service implementations MUST support the use of SAML V2.0 Metadata [SAML2Meta] in conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections. Additional expectations around the use of particular metadata elements related to profile behaviour may be encountered in those sections.	Prise en charge	
eGov 2.2.1 Metadata Profiles		
Implementations MUST support the SAML V2.0 Metadata Interoperability Profile Version 1.0 [MetaIOP].	Contrainte	Les mises en place de l'authentification électronique NE DOIVENT PAS utiliser la version 1.0 du Profil d'interopérabilité des métadonnées SAML V2.0 [MetaIOP].
In addition, implementations MUST support the use of the <md:KeyDescriptor> element as follows:	Prise en charge	
• Implementations MUST support the <ds:X509Certificate> element as input to subsequent requirements. Support for other key representations, and for other mechanisms for credential distribution, is OPTIONAL.	Contrainte	Aucun mécanisme FACULTATIF n'est pris en charge.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
• Implementations MUST support some form of path validation of signing, TLS, and encryption credentials used to secure SAML exchanges against one or more trusted certificate authorities. Support for PKIX [RFC5280] is RECOMMENDED; implementations SHOULD document the behaviour of the validation mechanisms they employ, particular with respect to limitations or divergence from PKIX [RFC5280].	Prise en charge	Les mises en place de l'authentification électronique DOIVENT respecter les exigences précisées à la section 2.4.5, Sécurité.
• Implementations MUST support the use of OCSP [RFC2560] and Certificate Revocation Lists (CRLs) obtained via the "CRL Distribution Point" X.509 extension [RFC5280] for revocation checking of those credentials.	Contrainte	Les mises en place de l'authentification électronique DOIVENT respecter les exigences précisées à la section 2.4.5, Sécurité.
• Implementations MAY support additional constraints on the contents of certificates used by particular entities, such as "subjectAltName" or "DN", key usage constraints, or policy extensions, but SHOULD document such features and make them optional to enable where possible.	Contrainte	Aucune contrainte supplémentaire FACULTATIVE n'est prise en charge.
Note that these metadata profiles are intended to be mutually exclusive within a given deployment context; they are alternatives, rather than complimentary or compatible uses of the same metadata information.	S.O.	

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Implementations SHOULD support the SAML V2.0 Metadata Extension for Entity Attributes Version 1.0 [MetaAttr] and provide policy controls on the basis of SAML attributes supplied via this extension mechanism.	Prise en charge	
eGov 2.2.2 Metadata Exchange		
It is OPTIONAL for implementations to support the generation or exportation of metadata, but implementations MUST support the publication of metadata using the Well-Known-Location method defined in section 4.1 of [SAML2 Meta] (under the assumption that entityID values used are suitable for such support).	Contrainte	L'Organe de gouvernance de la fédération des justificatifs du GC (OGFJGC) conserve et distribue les métadonnées à jour. Pour mettre un terme à l'utilisation de métadonnées non à jour par les membres de la fédération, l'OGFJGC interrompt la distribution de ces données. De plus, l'OGFJGC peut annuler un certificat dans le fichier de métadonnées, notamment en vue de mettre un terme à la participation d'un membre de la fédération ou encore en raison de la compromission d'un certificat et de changements de clé. • Les membres de la fédération DOIVENT présenter le document des métadonnées XML à l'OGFJGC. • Les membres de la fédération ne DOIVENT accepter que les documents de métadonnées XML qui proviennent de l'OGFJGC.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Implementations MUST support the following mechanisms for the importation of metadata: • local file • remote resource at fixed location accessible via HTTP 1.1 [RFC2616] or HTTP 1.1 over TLS/SSL [RFC2818] In the case of HTTP resolution, implementations MUST support use of the "ETag" and "Last-Modified" headers for cache management. Implementations SHOULD support the use of more than one fixed location for the importation of metadata, but MAY leave their behaviour unspecified if a single entity's metadata is present in more than one source.	Contrainte	L'Organe de gouvernance de la fédération des justificatifs du GC assure l'actualisation et la distribution des métadonnées à jour, comme on le décrit ci-dessus. Toute procédure additionnelle sera établie par l'OGFJGC.
Importation of multiple entities' metadata contained within an <md:EntitiesDescriptor> element MUST be supported.	Contrainte	L'importation de métadonnées d'entités multiples contenues dans un élément <md:EntitiesDescriptor> DOIT être prise en charge. L'Organe de gouvernance de la fédération des justificatifs du GC assure l'actualisation et la distribution des métadonnées à jour. S'il y a lieu, il est possible de modifier le processus de distribution de manière à permettre les logiciels de fournisseurs qui ne prennent pas en charge l'importation de métadonnées d'entités multiples contenues dans un élément <md:EntitiesDescriptor>.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Finally, implementations SHOULD allow for the automated updating/reimportation of metadata without service degradation or interruption.	Prise en charge	
eGov 2.2.2.1 Metadata Verification		
Verification of metadata, if supported, MUST include XML signature verification at least at the root element level, and SHOULD support the following mechanisms for signature key trust establishment: • Direct comparison against known keys. • Some form of path-based certificate validation against one or more trusted certificate authorities, along with certificate revocation lists and/or OCSP [RFC2560]. Support for PKIX [RFC5280] is RECOMMENDED; implementations SHOULD document the behaviour of the validation mechanisms they employ, particular with respect to limitations or divergence from PKIX [RFC5280].	Contrainte	• Les membres de la fédération DOIVENT signer leurs métadonnées à l'aide du certificat de signature remis par les services de gestion des justificatifs internes (GFI) du gouvernement. • Au moment de la consommation, le membre de la fédération qui fait appel aux métadonnées DOIT s'assurer que le certificat employé pour signer les métadonnées n'a pas été annulé. o Seules les Listes de certificats révoqués (LCR) sont prises en charge.
eGov 2.3 Name Identifiers		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
In conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections, Identity Provider and Service Provider implementations MUST support the following SAML V2.0 name identifier formats, in accordance with the normative obligations associated with them by [SAML2Core]: • urn:oasis:names:tc:SAML:2.0:nameid-format:persistent • urn:oasis:names:tc:SAML:2.0:nameid-format:transient	Contrainte	Les mises en place de l'authentification électronique DOIVENT prendre en charge les éléments persistants. Les mises en place de l'authentification électronique ne DOIVENT pas prendre en charge les éléments transitoires.
Support for other formats is OPTIONAL.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge d'autres formats.
eGov 2.4 Attributes		
In conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections, Identity Provider and Service Provider implementations MUST support the generation and consumption of <saml2:Attribute> elements that conform to the SAML V2.0 X.500/LDAP Attribute Profile [SAML-X500].	Contrainte	Les mises en place de l'authentification électronique DOIVENT respecter les exigences de la section 2.4.1, Attributs d'assertion requis.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
The ability to support <saml2:AttributeValue> elements whose values are not simple strings (e.g., <saml2:NameID>, or other XML values) is OPTIONAL. Such content could be base64-encoded as an alternative.	Contrainte	Les mises en place de l'authentification électronique DOIVENT respecter les exigences précisées à la section 2.4.1, Attributs d'assertion requis.
eGov 2.5 Browser Single Sign-On		
This section defines an implementation profile of the SAML V2.0 Web Browser SSO Profile [SAML2Prof].	Prise en charge	
eGov 2.5.1 Identity Provider Discovery		
Service Provider and Discovery Service implementations MUST support the Identity Provider Discovery Service Protocol Profile in conformance with section 2.4.1 of [IDPDisco].	Contrainte	Les mises en place de l'authentification électronique DOIVENT prendre en charge le profil de dépistage du fournisseur de services de justificatifs d'identité précisé dans le document [SAML2 Profils]. Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge le profil du protocole de service de dépistage du fournisseur de services de justificatifs d'identité précisé dans le document [SAML2 Dépistage].
eGov 2.5.2 Authentication Requests		
eGov 2.5.2.1 Binding and Security Requirements		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect binding [SAML2Bind] for the transmission of <saml2p:AuthnRequest> messages, including the generation or verification of signatures in conjunction with this binding.	Prise en charge	
Support for other bindings is OPTIONAL.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge d'autres liaisons.
eGov 2.5.2.2 Message Content		
In addition to standard core- and profile-driven requirements, Service Provider implementations MUST support the inclusion of at least the following <saml2p:AuthnRequest> child elements and attributes (when appropriate):	Contrainte	Tel que précisé ci-dessous.
• AssertionConsumerServiceURL	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS utiliser l'adresse URL AssertionConsumerService. • Le fournisseur de services de justificatifs d'identité tire cette information des métadonnées.
• ProtocolBinding	Contrainte	S'il est présent, l'attribut ProtocolBinding DOIT être « urn:oasis:names:tc:SAML:2.0:bindings: HTTP-POST ».

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
• ForceAuthn	Contrainte	On PEUT utiliser l'attribut ForceAuthn pour exiger que le fournisseur de services de justificatifs d'identité oblige l'utilisateur final à s'authentifier auprès du fournisseur, peu importe l'état de la session d'authentification de l'utilisateur dans le système du fournisseur de services de justificatifs d'identité. • Lorsqu'on utilise l'attribut ForceAuthn, le fournisseur de services de justificatifs d'identité ne doit pas changer son identificateur de nom par rapport à toute authentification précédente effectuée au cours de la session, même si cet identificateur est périmé. • Si on utilise l'attribut ForceAuthn et si l'authentification s'avère réussie, l'attribut AuthnInstant du fournisseur de services de justificatifs d'identité est réinitialisé pour l'utilisateur en question.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
• IsPassive	Contrainte	• L'attribut IsPassive PEUT être utilisé si le fournisseur de services ne souhaite pas que le fournisseur de services de justificatifs d'identité commande directement le navigateur de l'utilisateur (par exemple, afficher une page à l'intention de l'utilisateur). • Si l'attribut IsPassive est vrai, l'utilisateur DOIT être en mesure de s'authentifier de manière passive, sinon la réponse produite ne DOIT PAS comprendre d'attribut <Assertion>. • Cette caractéristique permet au fournisseur de services de déterminer s'il doit aviser l'utilisateur qu'il ou elle est sur le point d'interagir avec le fournisseur de services de justificatifs d'identité. Voici un exemple de situation passive : le fournisseur de services s'aperçoit, à l'aide du témoin du domaine commun, que l'utilisateur peut avoir une session en cours dans le système d'un fournisseur de services de justificatifs d'identité particulier.
• AttributeConsumingServiceIndex	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS préciser l'attribut AttributeConsumingServiceIndex.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
• <saml2p:RequestedAuthnContext>	Contrainte	• La demande d'authentification DOIT comprendre l'élément <RequestedAuthnContext>. • L'élément <RequestedAuthnContext> DOIT comprendre un niveau d'assurance, conformément aux précisions du document [SAML2 Assurance]. Les niveaux d'assurance de l'authentification électronique du gouvernement sont définis à la section 2.4.2 Niveaux d'assurance de l'authentification électronique du gouvernement. • Les fournisseurs de services DOIVENT demander un niveau d'assurance particulier à l'aide de l'opérateur de comparaison « exact ». • Le fournisseur de services PEUT demander plus d'un niveau d'assurance, par ordre de priorité. Cette particularité peut s'avérer utile si, par exemple, le niveau 2 est exigé mais si le fournisseur de services est disposé à accepter le niveau 3 dans les cas où le niveau 2 n'est pas possible.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
• <saml2p:NameIDPolicy>	Contrainte	• L'attribut <SPNameQualifier> PEUT être présent. o L'Organe de gouvernance de la fédération des justificatifs du GC (OGFJGC) peut établir des groupes d'affiliations de fournisseurs de services de la FJGC qui utiliseront des identifiants anonymes mais persistants (IAP). Dans ces cas-là, les fournisseurs de services PEUVENT utiliser l'attribut <SPNameQualifier> dans la demande d'authentification pour indiquer leur souhait d'utiliser un IAP commun. • L'attribut <NameIDPolicy> peut contenir l'attribut AllowCreate. o En général, la valeur de l'attribut AllowCreate est « vrai », de sorte que si l'utilisateur n'a jamais fait appel au fournisseur de services de justificatifs d'identité sélectionné pour accéder au fournisseur de services, un identificateur puisse être créé à son intention et des messages SAML puisse être échangés entre les parties. o Toutefois, il peut être utile de donner la valeur « faux »à l'attribut AllowCreate si le fournisseur de services souhaite désactiver le traitement de l'inscription de justificatifs dans l'interface utilisateur du fournisseur de services de justificatifs d'identité. • Si l'attribut Format est présent il DOIT

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Identity Provider implementations MUST support all <saml2p:AuthnRequest> child elements and attributes defined by [SAML2Core], but MAY provide that support in the form of returning appropriate errors when confronted by particular request options. However, implementations MUST fully support the options enumerated above, and be configurable to utilize those options in a useful manner as defined by [SAML2Core].	Prise en charge	
Implementations MAY limit their support of the <saml2p:RequestedAuthnContext> element to the value "exact" for the Comparison attribute, but MUST otherwise support any allowable content of the element.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT prendre en charge que la valeur « exact » pour l'attribut Comparison.
Identity Provider implementations MUST support verification of requested AssertionConsumerServiceURL locations via comparison to <md:AssertionConsumerService> elements supplied via metadata using case-sensitive string comparison. It is OPTIONAL to support other means of comparison (e.g., canonicalization or other manipulation of URL values) or alternative verification mechanisms.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT prendre en charge aucune autre méthode de comparaison.
eGov 2.5.3 Responses		
eGov 2.5.3.1 Binding and Security Requirements		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Identity Provider and Service Provider implementations MUST support the use of the HTTP-POST and HTTP-Artifact bindings [SAML2Bind] for the transmission of <saml2p:Response> messages.	Contrainte	Les mises en place de l'authentification électronique DOIVENT prendre en charge les liaisons HTTP POST. Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge les liaisons HTTP Artifact.
Support for other bindings, and for artifact types other than urn:oasis:names:tc:SAML:2.0:artifact-04, is OPTIONAL.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge d'autres liaisons.
Identity Provider and Service Provider implementations MUST support the generation and consumption of unsolicited <saml2p:Response> messages (i.e., responses that are not the result of a <saml2p:AuthnRequest> message).	Contrainte	Les mises en place de l'authentification électronique DOIVENT supprimer les messages <saml2p:Response> non sollicités. • Aucun cas d'utilisation de l'authentification électronique répertorié n'avait besoin de ces messages.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Identity Provider implementations MUST support the issuance of <saml2p:Response> messages (with appropriate status codes) in the event of an error condition, provided that the user agent remains available and an acceptable location to which to deliver the response is available. The criteria for "acceptability" of a response location are not formally specified, but are subject to Identity Provider policy and reflect its responsibility to protect users from being sent to untrusted or possibly malicious parties. Note that this is a stronger requirement than the comparable language in [SAML2Prof].	Prise en charge	Pour l'OGFJGC, « l'acceptabilité d'un emplacement de réponse » indique que les métadonnées ont enregistré l'élément <AssertionConsumerServiceURL>.
Identity Provider and Service Provider implementations MUST support the signing of <saml2:Assertion> elements in responses; support for signing of the <saml2p:Response> element is OPTIONAL.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge la signature de l'élément <saml2p:Response>.
Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the <saml2:EncryptedAssertion> element when using the HTTP-POST binding; support for the <saml2:EncryptedID> and <saml2:EncryptedAttribute> elements is OPTIONAL.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS installer le soutien FACULTATIF.
eGov 2.5.3.2 Message Content		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
The Web Browser SSO Profile allows responses to contain any number of assertions and statements. Identity Provider implementations MUST allow the number of <saml2:Assertion>, <saml2:AuthnStatement>, and <saml2:AttributeStatement> elements in the <saml2p:Response> message to be limited to one. In turn, Service Provider implementations MAY limit support to a single instance of those elements when processing <saml2p:Response> messages.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT envoyer que les messages <saml2p:Response> qui contiennent au moins un élément <saml2:Assertion> unique.
Identity Provider implementations MUST support the inclusion of a Consent attribute in <saml2p:Response> messages, and a SessionIndex attribute in <saml2:AuthnStatement> elements.	Contrainte	Les mises en place de l'authentification électronique par des FSJ ne DOIVENT PAS inclure un attribut Consent dans les messages <saml2p:Response> Il n'existe actuellement aucun cas d'utilisation de l'authentification
Service Provider implementations that provide some form of session semantics MUST support the <saml2:AuthnStatement> element's SessionNotOnOrAfter attribute.	Prise en charge	Pour connaître les contraintes imposées aux mises en place de l'authentification électronique du fournisseur de services de justificatifs d'identité, reportez-vous à la section 2.2

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Service Provider implementations MUST support the acceptance/rejection of assertions based on the content of the <saml2:AuthnStatement> element's <saml2:AuthnContext> element. Implementations also MUST support the acceptance/rejection of particular <saml2:AuthnContext> content based on the identity of the Identity Provider. [IAP] provides one such mechanism via SAML V2.0 metadata and is RECOMMENDED; though this specification is in draft form, the technical details are not expected to change prior to eventual approval.	Prise en charge	
eGov 2.5.4 Artifact Resolution		
Pursuant to the requirement in section 2.5.3.1 for support of the HTTP-Artifact binding [SAML2Bind] for the transmission of <saml2p:Response> messages, implementations MUST support the SAML V2.0 Artifact Resolution profile [SAML2Prof] as constrained by the following subsections.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge la liaison HTTP-Artifact.
eGov 2.5.4.1 Artifact Resolution Requests		
Identity Provider and Service Provider implementations MUST support the use of the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for the transmission of <saml2p:ArtifactResolve> messages.	S.O.	

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Implementations MUST support the use of SAML message signatures and TLS server authentication to authenticate requests; support for TLS client authentication, or other forms of authentication in conjunction with the SAML SOAP binding, is OPTIONAL.	S.O.	
eGov 2.5.4.2 Artifact Resolution Responses		
Identity Provider and Service Provider implementations MUST support the use of the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for the transmission of <saml2p:ArtifactResponse> messages.	S.O.	
Implementations MUST support the use of SAML message signatures and TLS server authentication to authenticate responses; support for TLS client authentication, or other forms of authentication in conjunction with the SAML SOAP binding, is OPTIONAL.	S.O.	
eGov 2.6 Browser Holder of Key Single Sign-On		
This section defines an implementation profile of the SAML V2.0 Holder-of-Key Web Browser SSO Profile Version 1.0 [HoKSSO].	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS prendre cette fonction en charge.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
The implementation requirements defined in section 2.5 for the non-holder-of-key profile apply to implementations of this profile.	S.O.	
eGov 2.7 SAML 2.0 Proxying		
Section 3.4.1.5 of [SAML2Core] defines a formalized approach to proxying the SAML 2.0 Authentication Request protocol between multiple Identity Providers. This section defines an implementation profile for this behaviour suitable for composition with the Single Sign-On profiles defined in sections 2.5 and 2.6.	Prise en charge	Les mises en place de l'authentification électronique DOIVENT prendre en charge cet aspect lorsqu'elles sont configurées de manière à agir à titre de fournisseur de services de justificatifs d'identité de mise en cache.
The requirements of the profile are imposed on Identity Provider implementations acting as a proxy. These requirements are in addition to the technical requirements outlined in section 3.4.1.5.1 of [SAML2Core], which also MUST be supported.	Prise en charge	Les mises en place de l'authentification électronique DOIVENT prendre en charge cet aspect lorsqu'elles sont configurées de manière à agir à titre de fournisseur de services de justificatifs d'identité de mise en cache.
eGov 2.7.1 Authentication Requests		
Proxying Identity Provider implementations MUST support the mapping of incoming to outgoing <saml2p:RequestedAuthnContext> and <saml2p:NameIDPolicy> elements, such that deployers may choose to pass through values or map between different vocabularies as required.	Prise en charge	Les mises en place de l'authentification électronique DOIVENT prendre en charge cet aspect lorsqu'elles sont configurées de manière à agir à titre de fournisseur de services de justificatifs d'identité de mise en cache.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Proxying Identity Provider implementations MUST support the suppression/eliding of <saml2p:RequesterID> elements from outgoing <saml2p:AuthnRequest> messages to allow for hiding the identity of the Service Provider from proxied Identity Providers.	Prise en charge	Les mises en place de l'authentification électronique DOIVENT prendre en charge cet aspect lorsqu'elles sont configurées de manière à agir à titre de fournisseur de services de justificatifs d'identité de mise en cache.
eGov 2.7.2 Responses		
Proxying Identity Provider implementations MUST support the mapping of incoming to outgoing <saml2:AuthnContext> elements, such that deployers may choose to pass through values or map between different vocabularies as required.	Prise en charge	Les mises en place de l'authentification électronique DOIVENT prendre en charge cet aspect lorsqu'elles sont configurées de manière à agir à titre de fournisseur de services de justificatifs d'identité de mise en cache.
Proxying Identity Provider implementations MUST support the suppression of <saml2:AuthenticatingAuthority> elements from outgoing <saml2:AuthnContext> elements to allow for hiding the identity of the proxied Identity Provider from Service Providers.	Prise en charge	Les mises en place de l'authentification électronique DOIVENT prendre en charge cet aspect lorsqu'elles sont configurées de manière à agir à titre de fournisseur de services de justificatifs d'identité de mise en cache.
eGov 2.8 Single Logout		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
This section defines an implementation profile of the SAML V2.0 Single Logout Profile [SAML2Prof]. For clarification, the technical requirements for each message type below reflect the intent to normatively require initiation of logout by a Service Provider using either the front- or back-channel, and initiation/propagation of logout by an Identity Provider using the back-channel.	Prise en charge	
eGov 2.8.1 Logout Requests		
eGov 2.8.1.1 Binding and Security Requirements		
Identity Provider implementations MUST support the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for the issuance of <saml2p:LogoutRequest> messages, and MUST support the SAML SOAP (using HTTP as a transport) and HTTP-Redirect bindings [SAML2Bind] for the reception of <saml2p:LogoutRequest> messages.	Prise en charge	
Service Provider implementations MUST support the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for both issuance and reception of <saml2p:LogoutRequest> messages.	Prise en charge	

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Support for other bindings is OPTIONAL.	Contrainte	Les mises en place de l'authentification électronique PEUVENT prendre en charge les liaisons http Redirect en vue de la production de messages <saml2p:LogoutRequest>. Aucune autre liaison n'est prise en charge.
Implementations MUST support the use of SAML message signatures and TLS server authentication to authenticate <saml2p:LogoutRequest> messages; support for TLS client authentication, or other forms of authentication in conjunction with the SAML SOAP binding, is OPTIONAL.	Contrainte	Les mises en place de l'authentification électronique DOIVENT respecter les exigences précisées à la section 2.4.5 Sécurité Sécurité
Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the <saml2:EncryptedID> element when using the HTTP-Redirect binding.	Prise en charge	
eGov 2.8.1.2 User Interface Behaviour		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Identity Provider implementations MUST support both user-initiated termination of the local session only and user-initiated Single Logout. Upon receipt of a <saml2p:LogoutRequest> message via a front-channel binding, Identity Provider implementations MUST support user intervention governing the choice of propagating logout to other Service Providers, or limiting the operation to the Identity Provider. Of course, implementations MUST return status information to the requesting entity (e.g. partial logout indication) as appropriate.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge les interventions de l'utilisateur qui régit la propagation de la fermeture de session à d'autres fournisseurs de services ou encore qui restreint le fonctionnement du fournisseur de services de justificatifs d'identité. • En tout temps, une demande de fermeture de session unique produit une fermeture de session globale pour la session principale.
Service Provider implementations MUST support both user-initiated termination of the local session only and user-initiated Single Logout.	Contrainte	Les mises en place de l'authentification électronique de fournisseur de services ne PEUVENT installer que le support de la fermeture de session unique (autrement dit la fermeture de session globale). • Les mises en place de l'authentification électronique de fournisseur de services de justificatifs d'identité DOIVENT propager la fermeture de session, sans intervention de la part de l'utilisateur, à tous les fournisseurs de services qui prennent part à la session et répondre au fournisseur de services initial.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Identity Provider implementations MUST also support the administrative initiation of Single Logout for any active session, subject to appropriate policy.	Prise en charge	L'OGFJGC indiquera s'il y a lieu, pour chaque mise en place de l'authentification électronique par des FSJ, quel soutien est nécessaire pour l'activation administrative de la fonction de fermeture de session unique.
eGov 2.8.2 Logout Responses		
eGov 2.8.2.1 Binding and Security Requirements		
Identity Provider implementations MUST support the SAML SOAP (using HTTP as a transport) and HTTP-Redirect bindings [SAML2Bind] for the issuance of <saml2p:LogoutResponse> messages, and MUST support the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for the reception of <saml2p:LogoutResponse> messages.	Contrainte	• Nota : Les liaisons HTTP Redirect utilisées pour l'envoi de messages <saml2p:LogoutResponse> sont à éviter et on ne doit les utiliser QUE SI le message <saml2p:LogoutRequest> a été envoyé à l'aide de cette liaison.
Service Provider implementations MUST support the SAML SOAP (using HTTP as a transport) binding [SAML2 Bind] for both issuance and reception of <saml2p:LogoutResponse> messages.	Prise en charge	
Support for other bindings is OPTIONAL.	Contrainte	Les mises en place d'authentification électronique ne DOIVENT PAS installer de prise en charge FACULTATIVE.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Implementations MUST support the use of SAML message signatures and TLS server authentication to authenticate <saml2p:LogoutResponse> messages; support for TLS client authentication, or other forms of authentication in conjunction with the SAML SOAP binding, is OPTIONAL.	Contrainte	Les mises en place d'authentification électronique ne DOIVENT PAS installer de prise en charge FACULTATIVE.
eGov 3 Conformance Classes		
eGov 3.1 Standard		
Conforming Identity Provider and/or Service Provider implementations MUST support the normative requirements in sections 2.2, 2.3, 2.4, and 2.5.	Prise en charge	
eGov 3.1.1 Signature and Encryption Algorithms		
Implementations MUST support the signature and digest algorithms identified by the following URIs in conjunction with the creation and verification of XML Signatures [XMLSig]: • http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 (defined in [RFC4051]) • http://www.w3.org/2001/04/xmlenc#sha256 (defined in [XMLEnc])	Prise en charge	Cette exigence s'applique aux algorithmes utilisés pour la signature des messages SAML à codage URL, comme le décrit la section 3.4.4.1 du document [SAML-Liaisons].

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Implementations SHOULD support the signature and digest algorithms identified by the following URIs in conjunction with the creation and verification of XML Signatures [XMLSig]: • http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256 (defined in [RFC4051])	Prise en charge	
Implementations MUST support the block encryption algorithms identified by the following URIs in conjunction with the use of XML Encryption [XMLEnc]: • http://www.w3.org/2001/04/xmlenc#tripledes-cbc • http://www.w3.org/2001/04/xmlenc#aes128-cbc • http://www.w3.org/2001/04/xmlenc#aes256-cbc	Prise en charge	Il faut utiliser des algorithmes cryptographiques approuvés par le CSTC pour l'authentification électronique et les logiciels d'autorisation, comme le précise le document ISTA-11. http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-fra.html (version actuelle).
Implementations MUST support the key transport algorithms identified by the following URIs in conjunction with the use of XML Encryption [XMLEnc]: • http://www.w3.org/2001/04/xmlenc#rsa-1_5 • http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p	Contrainte	Il n'existe actuellement aucun cas d'utilisation au sein du GC qui nécessite cette exigence.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Implementations SHOULD support the key agreement algorithms identified by the following URIs in conjunction with the use of XML Encryption [XMLEnc]: • http://www.w3.org/2009/xmlenc11#ECDH-ES defined in [XMLEnc11]) (This is a Last Call Working Draft of XML Encryption 1.1, and this normative requirement is contingent on W3C ratification of this specification without normative changes to this algorithm's definition.)	Prise en charge	Il faut utiliser des algorithmes cryptographiques approuvés par le CSTC pour l'authentification électronique et les logiciels d'autorisation, comme le précise le document ISTA-11. http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-fra.html (version actuelle).
Support for other algorithms is OPTIONAL.	Contrainte	Les AE mises en place ne DOIVENT prendre en charge AUCUN autre algorithme.
eGov 3.2 Standard with Logout		
Conforming Identity Provider and/or Service Provider implementations MUST meet the conformance requirements in section 3.1, and MUST in addition support the normative requirements in section 2.8.	Contrainte	Voir la section 2.8 ci-dessus.
eGov 3.3 Full		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Conforming Identity Provider and/or Service Provider implementations MUST meet the conformance requirements in section 3.1, and MUST in addition support the normative requirements in sections 2.6, 2.7, and 2.8.	Contrainte	• Il ne FAUT PAS configurer les authentifications électroniques mises en place d'après la section 2.6. • Les authentifications électroniques mises en place doivent plutôt être configurées en conformité avec la section 2.7 si elles doivent faire office de fournisseur de services de justificatifs d'identité de mise en cache.
End of table		

2.2 Autres contraintes visant les spécifications [SAML2*]

Outre les contraintes imposées par le présent Profil de mise en place quant au Profil eGov 2.0 [eGov 2.0] publié par l'initiative Kantara, le présent document de mise en place de l'authentification électronique stipule d'autres contraintes pour les spécifications SAML 2.0 sous-jacentes publiées par le Security Services Technical Committee (SSTC) d'OASIS.

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
[SAML2 Base] Section 2.7.2, ligne 1061 `<SessionNotOnOrAfter>`	Contrainte	La mise en place, par le fournisseur de services de justificatifs d'identité, de l'authentification électronique ne DOIT pas préciser l'attribut SessionNotOnOrAfter. Ainsi, le fournisseur de services peut fixer la durée voulue de son propre contexte de sécurité. • Si un fournisseur de services de justificatifs d'identité de la FJGC ne peut pas indiquer qu'il ne faut pas transmettre cette valeur, il doit alors préciser la valeur élevée fixée par l'OGFJGC.
[SAML2 Base] Section 3.2.1, ligne 1489 `<saml:Issuer>`	Contrainte	Demande d'authentification d'un fournisseur de services `<saml:Issuer>` • DOIT être présent. • DOIT être le code d'entité entity_id attribué par l'OGFJGC. •

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
[SAML2 Base] Section 3.4.1, ligne 2017 <saml:Subject>	Contrainte	La demande d'authentification d'un fournisseur de services <saml:Subject> : ne DOIT PAS être incluse. • Aucun cas d'utilisation de l'authentification électronique n'exige l'élément <saml:Subject>.
[SAML2 Base] Section 3.4.1, ligne 2029 <saml:Conditions>	Contrainte	La demande d'authentification d'un fournisseur de services <saml:Conditions> : ne DOIT PAS être incluse. • Aucun cas d'utilisation de l'authentification électronique n'exige l'élément <saml:Conditions>.
[SAML2 Base] Section 3.4.1, ligne 2068 ProtocolBinding	Contrainte	La demande d'authentification d'un fournisseur de services ProtocolBinding • PEUT être utilisée. • Si l'attribut ProtocolBinding est présent, il doit préciser : « urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST ».

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
[SAML2 Base] Section 3.6.1, ligne 2421 <ManageNameIDRequest>	Contrainte	Les mises en place des fournisseurs de services de justificatifs d'identité DOIVENT transmettre en temps opportun un élément <ManageNameIDRequest> avec <Terminate> dans le cas d'un justificatif qui a été révoqué, à tout fournisseur de services qui dispose d'un point de terminaison défini pour l'élément <ManageNameIDService> et pour lequel il a déjà envoyé une assertion pour l'utilisateur. Les mises en place des fournisseurs de services de justificatifs d'identité ne DOIVENT envoyer aucun autre message <ManageNameIDRequest>. Les mises en place des fournisseurs de services DOIVENT répondre aux messages <ManageNameIDRequest>.
		•
[SAML2 Liaisons] Section 3.5.3, ligne 785 <RelayState>	Contrainte	L'attribut <RelayState> ne PEUT PAS être adjoint à un message de réponse, sauf s'il a été fourni dans le message de demande correspondant.

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
[SAML2 Assurance] Section 3, ligne 276 <assurance-certification>	Contrainte	Les métadonnées des fournisseurs de services de justificatifs d'identité de l'authentification électronique DOIVENT préciser le ou les niveaux d'assurance pris en charge par l'attribut <assurance-certification>, selon la définition qui figure à la section 3, Identity Assurance Certification Attribute Profile (profil des attributs de certification de l'assurance de l'identité), du document [SAML2 Assurance]. La section 2.4.2, Niveaux d'assurance de l'authentification électronique du gouvernement, précisent les valeurs URI à utiliser pour les quatre niveaux d'assurance. Plusieurs valeurs de niveau d'assurance PEUVENT être précisées dans les métadonnées des fournisseurs de services d'identité, mais une seule valeur est renvoyée dans une réponse d'authentification.
[SAML2 Méta] Section 2.3.2, ligne 371 <entityID>	Contrainte	L'entité et l'OGFJGC DOIVENT convenir de l'attribut <entityID>.
[SAML2 Meta] Section 2.3.2.1, ligne 443 <Organization>	Contrainte	Il est PRÉFÉRABLE d'inclure l'attribut <Organization> et d'indiquer OrganizationName ou OrganizationDisplayName.

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
[SAML2 Méta] Section 2.3.2.2, ligne 476 <ContactPerson>	Contrainte	Il est PRÉFÉRABLE d'inclure l'attribut <ContactPerson>. L'authentification électronique propose d'ajouter l'adresse de courriel (EmailAddress) ou le numéro de téléphone (TelephoneNumber).
[SAML2 Méta] Section 2.4.1, ligne 550 <RoleDescriptor>	Contrainte	• L'élément de métadonnées <RoleDescriptor> ne DOIT PAS être utilisé.
[SAML2 Méta] Section 2.4.3, ligne 683 <IDPSSODescriptor> y compris la Section 2.4.2, ligne 643 <SSODescriptorType>	Contrainte	• L'attribut WantAuthnRequestsSigned DOIT indiquer la valeur « true ». • Deux attributs <SingleLogoutService> DOIVENT être présents (un pour chacune des liaisons : SOAP et HTTP Redirect). • Un seul attribut <SingleSignOnService> DOIT être présent. • Un seul attribut < ManageNameIDService> DOIT être présent en vue de la réception des réponses aux messages de terminaison NameID. La liaison précisée DOIT être : urn:oasis:names:tc:SAML:2.0:bindings:SOAP.

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
[SAML2 Méta] Section 2.4.4, ligne 736 <SPSSODescriptor> y compris la Section 2.4.2, ligne 643 <SSODescriptorType>	Contrainte	• L'attribut AuthnRequestsSigned DOIT indiquer la valeur « true ». • L'attribut WantAssertionsSigned DOIT indiquer la valeur « true ». • L'attribut <AssertionConsumerService> DOIT être inclus. • Un seul attribut <AssertionConsumerService> DOIT disposer de la liaison urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST. • Un seul attribut < ManageNameIDService> PEUT être présent pour indiquer l'envoi des messages de terminaison NameID par les fournisseurs de services d'identité. La liaison DOIT être : urn:oasis:names:tc:SAML:2.0:bindings:SOAP.
[SAML2 Méta] Section 2.4.5, ligne 828 <AuthnAuthorityDescriptor>	Contrainte	L'attribut <AuthnAuthorityDescriptor> ne DOIT PAS être utilisé.
[SAML2 Méta] Section 2.4.6, ligne 861 <PDPDescriptor>	Contrainte	L'attribut <PDPDescriptor> ne DOIT PAS être utilisé.

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
[SAML2 Méta] Section 2.5, ligne 938 <AffiliationDescriptor>	Contrainte	L'attribut <AffiliationDescriptor> PEUT être utilisé. • L'Organe de gouvernance de la fédération des justificatifs du GC (OGFJGC) peut établir des groupes d'affiliations de fournisseurs de services de la FJGC qui utiliseront des identifiants anonymes mais persistants (IAP). Dans ces cas-là. L'OGFJGC fournira des métadonnées définissant ces groupes.
[SAML2 MétaIU] Section 2.1.1 <md:UIInfo>	Prise en charge	Les métadonnées du fournisseur de services PEUVENT comprendre les éléments <mdui:DisplayName> et <mdui:Logo>. Le fournisseur de services de justificatifs d'identité PEUT utiliser ces éléments de métadonnées pour informer l'utilisateur au sujet de l'entité qui demande une authentification pendant le dialogue d'authentification associé.
Fin du tableau		

2.3 Autres extensions liées à la spécification [SAML2 *]

Outre les contraintes imposées par ce Profil de mise en place quant au Profil eGov 2.0 [eGov 2.0] publié par l'initiative Kantara, le présent document de mise en place de l'authentification électronique élargit également les spécifications SAML 2.0 sous-jacentes publiées par le Security Services Technical Committee (SSTC) d'OASIS.

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
Aucune exigence définie		
Fin du tableau		

2.4 Autres exigences du gouvernement

Outre les contraintes imposées par ce Profil de mise en place au Profil eGov 2.0 [eGov 2.0] publié par l'initiative Kantara, et les autres contraintes et extensions appliquées aux spécifications SAML 2.0 publiées par le Security Services Technical Committee (SSTC) d'OASIS, le présent document de mise en place de l'authentification électronique impose également d'autres exigences à l'environnement d'authentification électronique du gouvernement.

2.4.1 Attributs d'assertion requis

Exigence quant à l'authentification électronique	ASI STAE Prise en charge requise	Détails de la mise en place de l'authentification électronique
[SAML2 Base] Section 2.7.3, ligne 1165 `<AttributeStatement>`	Extension	Les mises en place de l'authentification électronique par les fournisseurs de services et les fournisseurs de services de justificatifs d'identité DOIVENT prendre en charge les attributs obligatoires de l'authentification électronique : • Ceux-ci sont indiqués à la section 2.4.1.1 Attributs obligatoires

Exigence quant à l'authentification électronique	ASI STAE Prise en charge requise	Détails de la mise en place de l'authentification électronique
[SAML2 Base] Section 2.7.3, ligne 1165 <AttributeStatement>	Extension	Les mises en place de l'authentification électronique par les fournisseurs de services de justificatifs d'identité PEUVENT prendre en charge des attributs facultatifs de l'authentification électronique : • Ceux-ci sont indiqués à la section 2.4.1.2 Attributs facultatifs
[SAML2 Base] Section 2.7.3, ligne 1165 <AttributeStatement>	Contrainte	Les mises en place de l'authentification électronique par les fournisseurs de services ne DOIVENT PAS prendre en charge la réception d'autres attributs. • Les mises en place de l'authentification électronique par les fournisseurs de services DOIVENT rejeter tout autre attribut et elles ne doivent pas utiliser les valeurs de ces attributs dans le traitement.
Fin du tableau		

2.4.1.1 Attributs obligatoires

Nom (URI)	Description	Format	Type de données
ca:gc:cyber-authentication:basic:specVer	Version de la spécification de l'interface	DOIT être « 2.0 » pour cette spécification d'interface [ASI STAE 2]	xs:chaîne

Nom (URI)	Description	Format	Type de données
Fin du tableau			

2.4.1.2 Attributs facultatifs

Nom (URI)	Description	Format	Type de données
ca:gc:cyber-authentication:basic:assuranceLevel	À éviter : n'est inclus que pour la transition depuis la version 1 de l'[ASI STAE 1] Degré de confiance du mécanisme d'authentification final.	DOIT être : 1, 2, 3, 4 ou test	xs:chaîne
urn:oid: 2.16.840.1.113730.3.1.39	À éviter : n'est inclus que pour la transition depuis la version 1 de l'[ASI STAE 1] Langue préférée de l'utilisateur final (celle-ci doit normalement être définie lorsque l'utilisateur change de langue pendant l'interaction avec le fournisseur de services de justificatifs d'identité).	DOIT être conforme à la définition du champ de l'en-tête Accept-Language défini, une exception prévalant cependant : la séquence "Accept-Language" ":" doit être omise.	xs:chaîne
Fin du tableau			

2.4.2 Niveaux d'assurance de l'authentification électronique du gouvernement

Les demandes et les réponses d'authentification sur les justificatifs de l'authentification électronique du gouvernement feront preuve du niveau d'assurance du gouvernement du Canada requis. Au total, quatre niveaux d'assurance sont définis dans [ITSG-31] et utilisés par le programme d'authentification électronique du gouvernement. Les valeurs des URI qui représentent ces niveaux d'assurance du gouvernement du Canada sont les suivantes :

- http://cyber-auth.gc.ca/assurance/loa1
- http://cyber-auth.gc.ca/assurance/loa2
- http://cyber-auth.gc.ca/assurance/loa3
- http://cyber-auth.gc.ca/assurance/loa4

Les schémas qui correspondent à ces valeurs sont offerts par l'OGFJ du gouvernement.

2.4.3 Communication des préférences linguistiques

Afin de respecter les exigences de la politique du gouvernement, il fallait disposer d'une méthode d'envoi de la langue préférée actuellement par l'utilisateur (et non celle du navigateur) du fournisseur de services au fournisseur de services de justificatifs d'identité et du fournisseur de services de justificatifs d'identité au fournisseur de services dans tous les cas, même dans les cas où l'authentification échoue et aucune assertion n'est produite. À cet égard, l'authentification électronique fait appel à un témoin de session qui figure dans un domaine commun défini par l'OGFJGC (il peut s'agir du même domaine que celui établi pour le profil de dépistage du fournisseur de services de justificatifs d'identité).

Ce témoin de session comprend l'attribut de langue, dont les valeurs sont définies dans le document [RFC 1766]. Les valeurs admises pour l'attribut de langue de l'authentification électronique sont indiquées ci-dessous:

- en (anglais)
- fr (français)

Les fournisseurs de services et les fournisseurs de services de justificatifs d'identité DOIVENT lire ce témoin et utiliser le paramètre de langue pour les pages d'interface utilisateur qui sont affichées.

Les fournisseurs de services et les fournisseurs de services de justificatifs d'identité DOIVENT veiller à ce que ce témoin précise la langue préférée de l'utilisateur avant de transmettre un message sur une liaison HTTP-Redirect ou HTTP-Post. Étant donné que ce

témoin de langue du gouvernement sera sans doute utilisé, que l'utilisateur se trouve ou non dans une situation de demande/réponse d'authentification, il doit être mis à jour dans les plus brefs délais.

Une annexe du présent document décrit les détails du témoin de langue du gouvernement dans le domaine commun.

2.4.4 Protocole de gestion d'identificateur de nom

Différents ministères du gouvernement exigent un avis en cas d'annulation de justificatif. Pour prendre cette fonction en charge, le document [ASI des STAE2] ajoute le soutien du protocole (et du profil) de gestion d'identificateur de nom SAML.

Les fournisseurs de services précisent s'ils souhaitent recevoir ces messages en adjoignant un élément <`ManageNameIDService`> à leur `SPSSODescriptor` dans les métadonnées du fournisseur de services.

Les FSJ DOIVENT envoyer une demande <`ManageNameIDRequest`> aux fournisseurs de services lorsqu'ils révoquent un code d'utilisateur utilisé auparavant par ces derniers. Les FSJ DOIVENT informer un fournisseur de services de l'annulation d'un code d'utilisateur (NameID) s'ils ont déjà transmis à ce fournisseur de services des assertions pour l'utilisateur visé, et ne DOIVENT PAS envoyer un tel avis d'annulation de code d'utilisateur NameID à d'autres fournisseurs de services. Les avis d'annulation doivent être transmis en temps opportun via le canal d'appui, selon une méthode approuvée par l'OGFJGC. À cette fin, les FSJ DOIVENT ajouter un élément <`ManageNameIDService`> à leur descripteur `IDPSSODescriptor` dans leurs métadonnées. La STAE2 utilise des identificateurs anonymes mais persistants (IAP), c'est-à-dire des identificateurs persistants SAML [SAML2 BASE, 3.7] et [SAML2 Errata, E78].. Pour cette raison, les FSJ doivent attribuer « …un identificateur opaque persistant à chaque utilisateur... ». Par ailleurs, « une valeur donnée, une fois associé à un utilisateur, NE DOIT JAMAIS être attribué à un autre utilisateur ».

2.4.5 Sécurité

Pour établir des communications fiables et sûres, cette spécification d'interface est largement tributaire des paires de clés cryptographiques X.509v3. La présente section décrit les différents certificats nécessaires ainsi que les détails de l'utilisation de ceux-ci.

2.4.5.1 Certificats des Services de gestion des justificatifs internes (GFI) du gouvernement

Les Services de gestion des justificatifs internes (GFI) du gouvernement, qui sont exploités par TPSGC pour le compte du gouvernement, assurent la fiabilité et la sécurité de la fédération des justificatifs du gouvernement. Toute interopération au sein de la fédération des justificatifs du GC nécessite la possession de certificats valides émis par les services de GFI. Les services de GFI remettent trois certificats à chaque fournisseur de services (un est utilisé pour TLS, un pour la signature numérique et un troisième

pour le chiffrement) et deux certificats à chaque fournisseur de services de justificatifs d'identité (un pour TLS et un autre pour la signature numérique).

- Ces certificats DOIVENT être conservés en conformité avec les responsabilités de l'abonné (que précise l'OGFJGC).

2.4.5.2 Signature numérique

Les expéditeurs de tous les messages SAML, et des parties de ceux-ci, DOIVENT signer ces messages à l'aide du certificat de signature des services de GFI du gouvernement qui leur a été remis. À l'aide de la signature, le destinataire du message peut authentifier l'expéditeur et confirmer que le message n'a pas été modifié depuis l'apposition de la signature.

- Une fois qu'il a reçu le message, le destinataire DOIT authentifier l'expéditeur et vérifier la signature.
- Le destinataire DOIT vérifier si le certificat de l'expéditeur qui a servi à signer le message a été annulé. Pour effectuer cette vérification, les systèmes membres de la fédération DOIVENT utiliser la méthode ci-dessous :
    - Liste de certificats révoqués (LCR) – L'emplacement de la LCR (dans le répertoire ou au site Web) peut être configuré de manière fixe dans le logiciel; la LCR est par la suite téléchargée périodiquement. Pour obtenir plus de détails sur l'emplacement des noms distinctifs et le nom d'hôte du répertoire, veuillez consulter la documentation sur le GFI du GC de l'OGFJGC.
- Si l'état du certificat (annulé ou non) ne peut pas être déterminé, le système membre de la fédération DOIT rejeter le message correspondant.

2.4.5.3 Chiffrement

Le chiffrement permet de s'assurer que seul le destinataire prévu est en mesure de déchiffre le message et lire l'information confidentielle qu'il renferme.

- Toute l'information confidentielle d'un message SAML DOIT être chiffrée.
- Le chiffrement DOIT utiliser la clé publique du certificat de chiffrement remis par les services de GFI du gouvernement au destinataire prévu.

2.4.5.4 Sites Web de TLS

2.4.5.4.1 Pour les liaisons de canal d'avant-plan

Cette spécification d'interface précise les liaisons de canal d'avant plan qui utilisent http sur TLS (HTTPS) pour la transmission des messages.

- Les sites gérés par les membres de la fédération qui utilisent les liaisons HTTP sur TLS DOIVENT doivent protéger les sessions TLS à l'aide d'un certificat accepté par défaut par les navigateurs commerciaux.
- L'utilisation de SSLv3.0/TLS doit être conforme aux lignes directrices du CST (par exemple ASTI-11G) et aux politiques ministérielles.
- La liaison HTTPS sur TLS (v1.1 ou supérieure) DOIT être utilisée, sauf si elle n'est pas prise en charge par le navigateur.
- La liaison HTTPS sur TLS (v1.0) PEUT être utilisée.
- La liaison HTTPS sur SSL (v3.0 ou supérieure) ne PEUT être utilisée que si le protocole TLS (v1.0 ou supérieure) n'est pas pris en charge par le navigateur.
- Les versions antérieures du protocole SSL ne DOIVENT PAS être utilisées.

2.4.5.4.2 Pour les liaisons de canal d'appui

Cette spécification d'interface précise les liaisons de canal d'appui qui utilisent SOAP sur TLS pour le transport des messages.

- Les sites gérés par les membres de la fédération qui utilisent les liaisons SOAP sur TLS DOIVENT doivent protéger les sessions TLS à l'aide d'un certificat remis par les services de GFI du gouvernement.
- L'utilisation de SSLv3.0/TLS doit être conforme aux lignes directrices du CST (par exemple ASTI-11G) et aux politiques ministérielles.
- Le protocole TLS (v1.1 ou supérieure) 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 de l'interface d'authentification électronique requise	Détails de la mise en place de l'authentification électronique
Le service SAML d'un membre de l'authentification électronique DOIT traiter les erreurs sans accroc.	Plus particulièrement, le service SAML d'un membre de l'authentification électronique DOIT traiter la liste des erreurs possibles indiquées à la section 2.4.6.1, Erreurs à traiter .

2.4.6.1 Erreurs à traiter

Le tableau ci-après présente les erreurs que le service SAML d'un membre de l'authentification électronique DOIT traiter sans accroc (autrement dit d'une façon conviviale et contrôlée, conformément à la capacité du fournisseur de services de justificatifs d'identité ou du fournisseur de services de répondre). Le tableau catégorise les erreurs d'après les événements SAML.

Erreur
Erreur dans le traitement de la <Response> (réponse) • <Issuer> (expéditeur) incorrect ou inconnu • Version incorrecte • Incorrect Version • InResponseTo (en réponse à) non reconnu • IssueInstant (envoi) inacceptable • L'état indiqué n'est pas la réussite

Erreur dans le traitement de l'<Assertion> • Signature non valide • Certificat de signature révoqué • Impossible de déterminer l'état quant à la révocation • La durée de l'<Assertion> n'est pas valide • Impossible de déchiffrer l'<Assertion> • Destinataire incorrect • Version incorrecte
Erreur dans le traitement de <AuthnRequest> (demande d'authentification) • <Issuer> (expéditeur) inconnu • Signature non valide • Certificat de signature révoqué • Impossible de déterminer l'état quant à la révocation
Erreur dans le traitement de la demande de fermeture de session unique • <Issuer> (expéditeur) inconnu • Signature non valide • Certificat de signature révoqué • Impossible de déterminer l'état quant à la révocation

Erreur dans le traitement de la <Response> (réponse) SLO

- <Issuer> (expéditeur) inconnu
- Signature non valide
- Certificat de signature révoqué
- Impossible de déterminer l'état quant à la révocation

Annexe A: Autres fonctions en plus de l'authentification électronique (normatives)

A.1. Témoin de langue du GC

On présente ci-après une méthode à l'aide de laquelle le fournisseur de services ou le fournisseur de services de justificatifs d'identité peut déterminer la langue dont se sert actuellement l'utilisateur. Cette méthode fait appel à un témoin qui est stocké dans un domaine commun aux fournisseurs de services de justificatifs d'identité et aux fournisseurs de services dans la mise en place de la FJGC. Ce domaine est établi par l'OGFJGC et il peut être le même que le domaine commun utilisé pour le profil de dépistage du fournisseur de services de justificatifs d'identité; dans ce profil il s'appelle <common-domain> et le témoin qui renferme la dernière langue utilisée est le témoin de langue du GC.

Dans la FJGC, le fournisseur de services et le fournisseur de services de justificatifs d'identité doivent héberger des serveurs Web dans le domaine commun, comme l'indique l'OGFJGC.

A.1.1 Témoin de langue du GC stocké dans un domaine commun du GC

Le nom du témoin DOIT être « _gc_lang ». Le format de la valeur du témoin DOIT être celui d'une chaîne de texte monovaluée.

Le service de stockage de témoin dans le domaine commun (voir ci-après) DOIT mettre à jour le paramètre de langue si l'utilisateur indique une autre langue. Il s'agit ainsi que la dernière langée précisée figure dans le témoin. Les valeurs du témoin de langue du GC sont définies dans le document [RFC 1766]. Les valeurs acceptables pour le témoin de langue du GC sont les suivantes :

- en (anglais)
- fr (français)

Le témoin défini DOIT comporter le préfixe de chemin « / ». Le domaine précisé DOIT être « .<common-gc-domain> », <commun-gc-domaine> étant le domaine commun du GC établi par l'OGFJGC pour cette méthode (on peut également l'utiliser avec le profil de dépistage du fournisseur de services de justificatifs d'identité). Un point doit figurer au début. Le témoin DOIT être désigné comme étant sûr.

La syntaxe du témoin doit être conforme au document RFC 2965 de l'IETF. Le témoin ne DOIT concerner que la session en cours.

A.1.2 Obtention du témoin de langue du GC

Avant de présenter un dialogue d'authentification à l'utilisateur, le fournisseur de services de justificatifs d'identité DOIT connaître la langue choisir par cet utilisateur pour les communications. À cet égard, le fournisseur de services de justificatifs d'identité DOIT lancer un échange destiné à présenter le témoin de langue du GC au fournisseur de services de justificatifs d'identité après qu'il ait été lu par un serveur HTTP du domaine commun.

La méthode à l'aide de laquelle le fournisseur de services lit le témoin est propre à la mise en œuvre, pourvu que celle-ci soit en mesure d'amener l'agent de l'utilisateur à présenter des témoins qui ont été définis d'après les paramètres appropriés. Une stratégie de mise en œuvre acceptable est décrite ci-dessous; il ne s'agit pas d'une stratégie normalisée. De plus, elle peut ne pas être optimale pour certaines applications.

- Le fournisseur établit au préalable un pseudonyme DNS et IP à son intention dans le domaine commun.
- Renvoyer l'agent de l'utilisateur à lui-même à l'aide du pseudonyme DNS, à l'aide d'une URL qui précise « http » à titre de schéma URL. La structure de l'URL est propre à la mise en œuvre et elle peut comprendre l'information sur la session qui sert à identifier l'agent de l'utilisateur.
- Renvoyer l'agent de l'utilisateur, cette fois à lui-même.

A.1.3 Définition du témoin de langue du GC

Avant d'appeler une demande d'authentification, le fournisseur de services DOIT s'assurer que le témoin de langue du GC précise la langue choisir par l'utilisateur. Avant d'envoyer une réponse d'authentification électronique (y compris les réponses d'erreur), le fournisseur de services de justificatifs d'identité DOIT veiller à ce que le témoin de langue du GC soit défini en fonction de la langue choisie par l'utilisateur. Le fournisseur de services ou le fournisseur de services de justificatifs d'identité PEUT redéfinir le témoin de langue du GC si l'utilisateur change la langue. La méthode par laquelle le fournisseur de services le fournisseur de services ou le fournisseur de services de justificatifs d'identité définit le témoin est propre à la mise en œuvre, pourvu que le témoin soit défini correctement selon les paramètres indiqués ci-dessus. Une stratégie de mise en œuvre acceptable est présentée ci-dessous. Il ne s'agit pas d'une stratégie normalisée. Le fournisseur de services ou le fournisseur de services de justificatifs d'identité peut :

- Établir au préalable un pseudonyme DNS et IP à son intention dans le domaine commun.
- Renvoyer l'agent de l'utilisateur à lui-même à l'aide du pseudonyme DNS, à l'aide d'une URL qui précise « http » à titre de schéma URL. La structure de l'URL est propre à la mise en œuvre et elle peut comprendre l'information sur la session qui sert à identifier l'agent de l'utilisateur.
- Définir le témoin de l'agent de l'utilisateur renvoyé à l'aide des paramètres précisés ci-dessus.
- Renvoyer l'agent de l'utilisateur, cette fois à lui-même.