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

Better government: with partners, for Canadians

Cyber Authentication Technology Solutions Interface Architecture and Specification Version 2.0: Deployment Profile

Status: Baseline for RFP #3
Final r7
Date modified: 14 December, 2010 16:18
File name: CA - CATS IA&S V2.0_Deployment Profile_Final r7_en.doc

For further information contact:
Bob Sunday
Cyber-Authentication Program
Chief Information Officer Branch
Treasury Board Secretariat
613-941-4764
Email: robert.sunday@tbs-sct.gc.ca

To be Approved by: TBS, CIO

Cyber-Auth ADM Committee

Canada

Revision Record Sheet

VERSION NO.	DESCRIPTION	DATE ISSUED	Status	AUTHOR & NOTES
0.1	Initial text	17th September 2010	Early Draft - Work in Progress	Bob Sunday, TBS
0.2	Draft to be reviewed for Approval at 28th October RFP #3 Tiger Team Workshop	4th October 2010	First Draft	Bob Sunday, TBS
draft r4	Recommended Document for approval by governance as Baseline document.	15th November 2010	Recommended Baseline	Bob Sunday, TBS With a lot of help from the RFP #3 Tiger Team and their colleagues
draft r5	Recommened Baseline document to be approved by Cyber-Auth DG Coimmittee	19th November 2010	Recommended Baseline	Bob Sunday, TBS
Final r6	Finalized Baseline document to be attached to the draft RFP #3	25th November 2010	Baseline for RFP #3	Bob Sunday, TBS
Final r7	Finalized Baseline document to be attached to the draft RFP #3	14th December 2010	Baseline for RFP #3	Bob Sunday, TBS

Foreword

Release Note for this version Final r7

This "*Cyber Authentication Technology Solutions - Interface Architecture and Specification - Version 2.0: Deployment Profile*" is the Finalized Baseline revision to the "*Cyber-Auth Tactical Solution (CATS) Interface Architecture and Specification*". This version is the "official" baseline document approved for distribution with RFP #3 by the Cyber-Auth DG Committee at its meeting on 23rd November, 2010.

Subsequent changes to this baseline document will be processed with official change requests and dispositions.

Table of Contents

1 Introduction

1.1 The Cyber Authentication Program Vision

The Cyber Authentication Program at the Government of Canada has a Vision which is partially described in the following diagram:

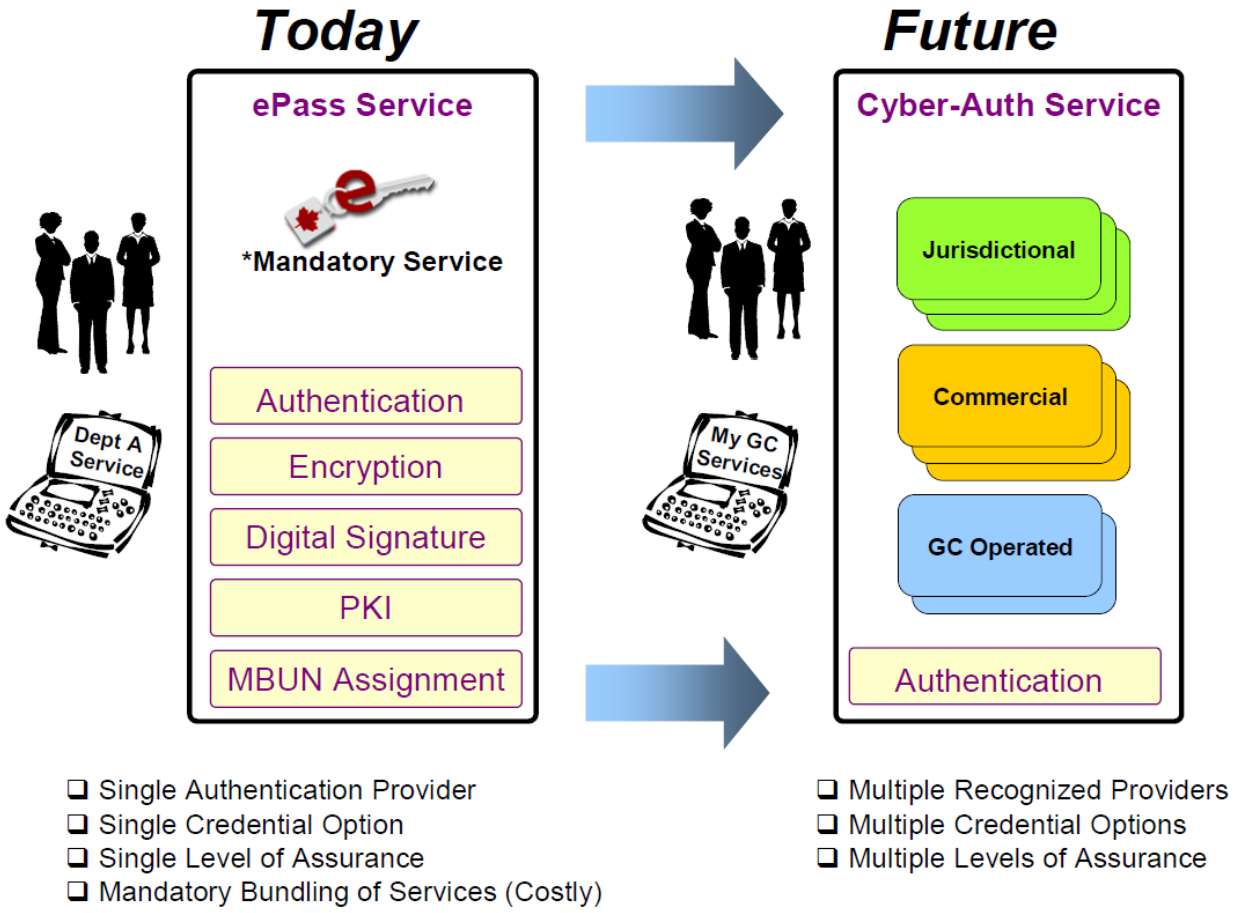

Figure 1: Cyber-Auth Vision

Further detail on the Cyber-Auth Vision can be found in other documents such as [CA-Program]

1.2 Overview of the CATS2 IA&S Deployment Profile

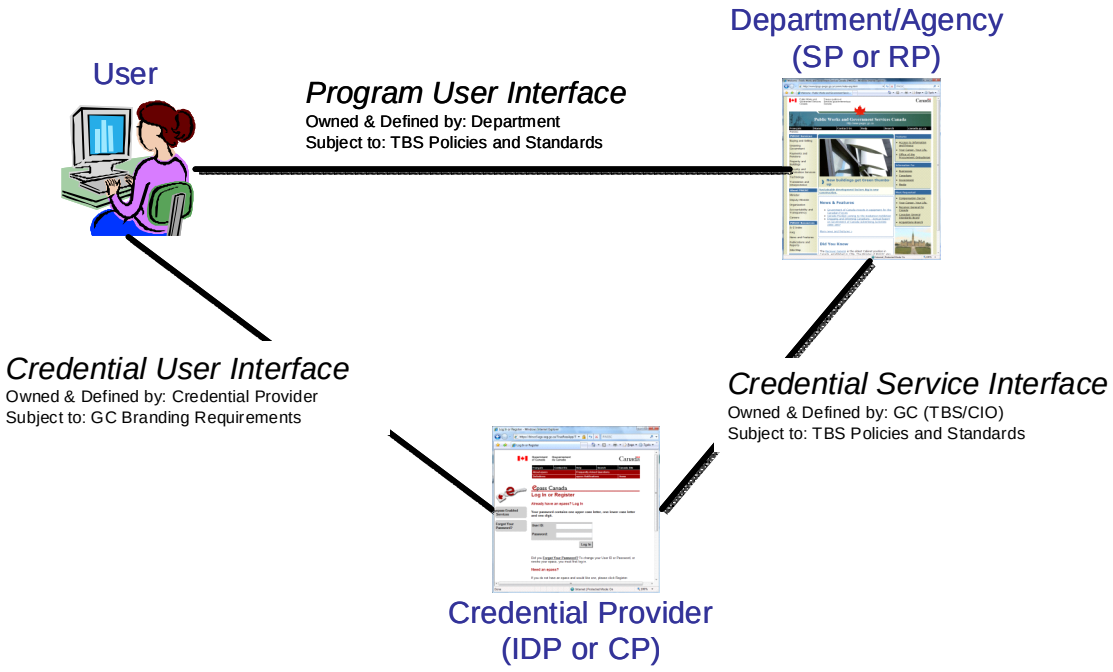

Figure 2: Business View of Authentication Interfaces

This "*CATS2 IA&S Deployment Profile*" [CATS2 IA&S] is a deployment level profile for participation in the Government of Canada's Cyber-Auth environment. It describes the messaging interface referred to as the Credential Service Interface in Figure 2: Business View of Authentication Interfaces

It applies to deployments configured to participate as both Service Providers (SPs) and Identity Providers (IDPs). In the GC context, SPs are also called Relying Parties (RPs), typically departmental online services, and IDPs are called Credential Providers (CPs).

NOTE: In this document we use the terminology of SP and IDP. Other Cyber-Auth documents may use the terms RP and CP. SAML and Kanatara Initiative documentation use the terms SP and IDP.

This deployment profile is an evolution of the former GC document "*Cyber-Auth Tactical Solution (CATS) Interface Architecture and Specification*" [CATS1 IA&S].

This deployment profile is not a tutorial or guidance document. Further guidance and use cases can be found in documents such as [CA-ConOps].

1.3 Compliance to CATS2 IA&S Deployment Profile

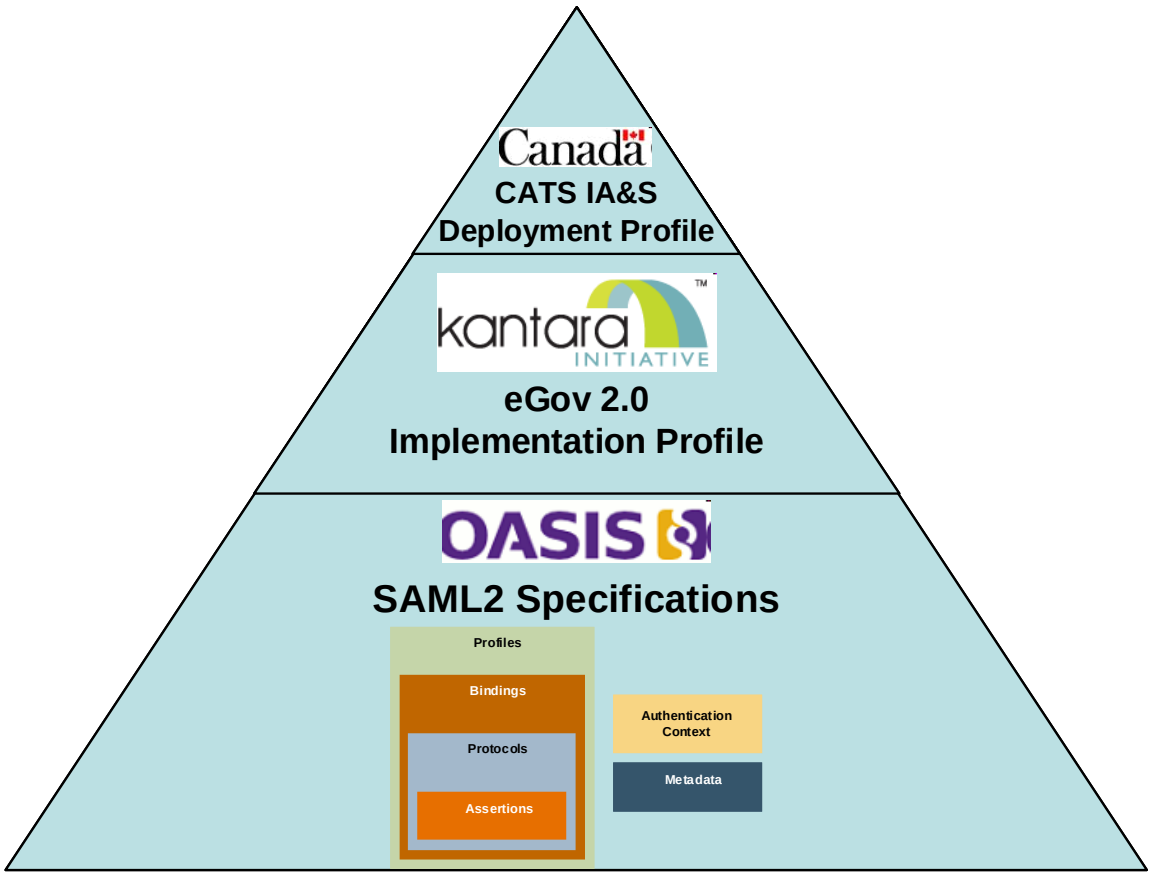

Figure 3: The Cyber-Auth Interface Architecture Building Blocks

This deployment profile is based on but does not require full compliance with the eGov 2.0 Profile [eGov 2.0] published by the Kantara Initiative. The normative requirements of this GC Deployment Profile in terms of the applicable sections of the eGov 2.0 Profile are detailed in Section 2 of this document. The eGov 2.0 Profile is based on the SAML 2.0 specifications created by the Security Services Technical Committee (SSTC) of OASIS. The eGov 2.0 Profile constrains the base SAML 2.0 features, elements, attributes and other values required for approved eGovernment federations and deployments. Unless otherwise specified, SAML operations and features follow those found in the OASIS SAML 2.0 specifications [SAML2 *].

NOTE: Interoperability testing conducted by external bodies, such as the Kantara Initiative, may assist confirmation of compliance. As such, GC acquisitions which require compliance with this deployment profile may also require the underlying software to comply with external interoperability testing.

However, these external tests do not form a complete and final confirmation of compliance with these GC deployment requirements. Additional testing may be required by the GC Credential Federation Governance Body (GCCFGB) to allow participation in the GCCF.

1.4 Changes from the *CATS1 Interface Architecture and Specification*

This document differs from the [CATS1 IA&S] in a number of areas:

These changes are generally described below; the full detailed normative conformance requirements for this deployment profile are specified within this document in Section 2 titled: "Deployment Requirements (Normative)"

1.4.1 Focus is on deployment rather than underlying technology

This deployment profile document relaxes the rules (but not the conformance requirements) that have previously required the underlying software products at the SPs and IDPs to have passed Liberty Alliance Interoperability testing.

The new rules will require the deployment of the IDP "Service" and the SP "Service" to be interoperability tested and certified against the rules in this deployment profile document.

Kantara Initiative test plan documents identify many test cases that are useful in testing many sections of this deployment profile and these will greatly assist the GCCF in determining conformance. Also, using COTS software that has passed the Liberty Alliance or Kantara Initiative Interoperability testing will greatly improve the chances of successfully meeting these deployment requirements.

This change of focus means that the GC Credential Federation Governance Body (GCCFGB) will be the authoritative body to determine whether a deployment (SP or IDP) has been sufficiently tested for the service to become a member of the federation.

1.4.2 Support of Level of Assurance is explicitly required

The GCCF supports multiple Levels of Assurance (LoAs) and therefore, stating desired LoA (by SP) and provided LoA (by IDP) is required. Support for Level of Assurance is required as specified in [SAML2 Assur]. The GC Cyber-Auth LoA's are described in [ITSG-31] and the associated URI's are specified in this *"CATS IA&S Deployment Profile"* in Section 2.4.2, GC Cyber-Auth Levels of Assurance.

SPs MUST request a specific Level of Assurance with the "exact" compare operator. Note that the SP may state that more than one LoA is acceptable. E.g. this is useful when a level 2 is required but the SP is willing to accept (and perhaps pay for) a level 3 if a level 2 is not possible.

IDPs MUST provide the exact LoA requested and MUST reject any LoA request that is not defined as a GC Cyber-Auth LoA. IDPs that are not configured to support the LoA requested MUST reject the authentication request with an appropriate status code.

The Metadata requirements include additional support for Level of Assurance as specified in [SAML2 Assur].

1.4.3 Authentication responses MUST be returned

Existing COTS products differ in their ability to send Authentication responses in certain circumstances while processing the <AuthnRequest>. In CATS1 deployments this led to an inadequate user experience (e.g. when user cancelled login).

The Kantara Initiative eGov 2.0 Profile [eGov 2.0] now requires that responses be produced and sent regardless of the success or failure of the <AuthnRequest>. This requirement is supported by this *"CATS2 IA&S Deployment Profile"* and will lead to improved user messaging and better continuity of user dialogue.

1.4.4 IDP Discovery MUST be implemented

In a single credential provider environment there was no need to choose which credential provider the user wished to go to. Thus, the CATS1 requirement for the IDP Discovery Profile to allow the user to choose their credential provider was deferred for both SPs and IDPs

With the GC environment now supporting multiple IDPs, a mechanism to support the SP and the user in choosing the IDP was necessary.

This *"CATS2 IA&S Deployment Profile"* does not change the specification in [CATS1 IA&S], but it does mandate that now the IDP Discovery Profile must be included in the deployment. This may require changes at existing SPs and IDPs.

1.4.5 Single Logout uses parallel back-channel requests

Existing deployments support Single Logout using SAML front-channel bindings. This requires sending the user's browser to each SP in turn (i.e. serialization of the logouts at each SP). It also increases the probability that an error will cause the user to be left in an uncertain state.

To improve this situation, CATS2 adds the support for parallel back-channel bindings to handle Single Logout. This adds support for SOAP bindings for Logout Requests and Responses as specified in the eGov 2.0 Profile [eGov 2.0].

The department can now choose between:

- Retaining control of the user session while instructing the IDP to logout the user.
- Passing control of the user session to the IDP
    - to give the IDP the ability to inform the user of specific error situations that may arise and on completion returning the user to the SP.

1.4.6 Language passing uses a GC Language Cookie

The Government of Canada's Official Languages Act (OLA) and Common Look and Feel Policy require a way to communicate the user's current language preference in all cases, even when authentication fails and an assertion is not produced.

CATS1 did not have a way to send the user's current language to the IDP. So, GC Access Key had to present a bilingual 1st page and was not able to return any change of language when authentication did not succeed. This did not fully meet the requirements of the OLA.

Cyber-Auth in CATS2 now does this by utilizing a GC Language Cookie. This session based cookie will be updated and read by SPs and IDPs whenever knowledge of language is required to meet the GC OLA.

Note: While this facility is needed for Cyber- Authentication, its use is applicable to other situations in the GC, such as Portals. To allow it to be placed in a more relevant future GC standard, it has been specified in a generic way and placed in an appendix in this document.

1.4.7 Notification of Credential Revocation

When a credential provider revokes a credential that has been in use in a department, there is no method in CATS1 for the department to be notified. A number of GC Departments require this capability to manage their enrolments.

CATS2 adds support for the IDPs to send this information in back-channel requests using the SAML Name Identifier Management Protocol (and Profile).

These enhancements allow SPs to specify their desire for receiving these messages through Metadata and also require IDPs to notify SPs in the event that a credential previously used at the SP has been revoked. IDPs are only required to send these NameID termination messages to SPs for whom they have previously sent assertions for the same principal.

1.4.8 A Number of Miscellaneous Corrections/Updates

A number of miscellaneous corrections/updates are required:

- To properly handle PAI's that are sent to multiple departments, `<NameID>` in the assertion must include `SPNameQualifier`. This fixes a bug in CATS1.
- All logouts will be global. That is, all logouts will generate a full Single Logout profile across all SPs involved in the user's session. There will no longer be a requirement for the IDP or the SP to propose local versus global logout. This fixes a usability problem.
- `RelayState` MUST not be returned in an Authentication Response message unless it was received in the corresponding Authentication Request message. This fixes a bug in CATS1.
- `SessionNotOnOrAfter` should not be returned in an Authentication Response message in order for the SP to determine its own timeout duration. This fixes a usability problem.
- The SP's logo and display name will be added to the SP's Metadata. This positions CATS2 for possible co-branding requirements.

1.5 Document References

[CA-ConOps] To be produced

[CA-Glossary] To be produced

[CA-Program] To be produced

[CATS1 IA&S] "Cyber-Auth Tactical Solution Interface Architecture and Specification Version 1.0" dated 23 January, 2009

[CATS2 IA&S] This document "*Cyber-Auth Technology Solutions Interface Architecture and Specification Version 2.0: Deployment Profile*"

[eGov 2.0] "Kantara Initiative eGovernment Implementation Profile of SAML V2.0 Version 2.0" available from http://kantarainitiative.org/confluence/download/attachments/42139782/kantara-egov-saml2-profile-2.0.pdf

[ITSG-31] "IT Security Guidance: User Authentication Guidance for IT Systems" published by Communications Security Establishment Canada and available from http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/index-eng.html

[RFC 1766] Tags for the Identification of Languages http://www.ietf.org/rfc/rfc1766.txt

[SAML2 *] All the SAML2 document references are available at http://docs.oasis-open.org/security/saml/v2.0 or alternatively at http://wiki.oasis-open.org/security/FrontPage

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

[SAML2 Conf] OASIS Standard, Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf

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

[SAML2 Discov] OASIS Committee Specification 01, Identity Provider Discovery Service Protocol and Profile, March 2008. http://www.oasis-open.org/committees/download.php/28049/sstc-saml-idp-discovery-cs-01.pdf

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

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

[SAML2 MetaUI] OASIS Working Draft 06, Metadata Extensions for Login and Discovery

User Interface Version 1.0, November 2010
http://www.oasis-open.org/committees/download.php/40270/sstc-saml-metadata-ui-v1.0-wd06.pdf

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

1.6 Glossary and Acronyms

See [CA-Glossary] for definition of the following terms and acronyms:

- Credential
- Persistent Anonymous Identifier (PAI)
- GCCF
- GCCFGB
- URI

2 Deployment Requirements (Normative)

2.1 Constraints on the Kantara Initiative eGov 2.0 Profile

This specification builds upon the SAML 2.0 suite of specifications [SAML2 *] and the profile of SAML2 referred to as Kantara Initiative eGovernment Implementation Profile of SAML2 version 2.0 [eGov 2.0]

This deployment profile is based on but does not require full compliance with the eGov 2.0 Profile [eGov 2.0] published by the Kantara Initiative (see the note in Section 1.3 on page 4). While the Kantara eGov 2.0 profile is an "implementation" profile for vendors of software products, this Cyber-Auth profile is a "deployment" profile which further constrains and explains the deployment of Service Providers and Credential Providers in the GC Cyber-Auth environment. Where this *"CATS2 IA&S Deployment Profile"* does not explicitly provide SAML2 guidance, one must implement in accordance with applicable OASIS SAML 2.0 requirements

The following table is in the order and description of the requirements in [eGov 2.0], Sections 2 & 3 which are repeated word for word in the first column. The table is annotated with the support required by the GC Cyber-Auth Program: typically this is either "Support" or "Constrained" or "n/a" (not applicable). Whenever further details are required to fully explain the GC requirement, they are provided in the 3rd column.

There are also requirements which are additional to these eGov 2.0 requirements and they are specified in the subsequent sections. Cyber-Auth also has constraints on the SAML v2.0 specifications and has a few Cyber-Auth specific requirements

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
2.2 Metadata and Trust Management		
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 behavior may be encountered in those sections.	Support	

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
2.2.1 Metadata Profiles		
Implementations MUST support the SAML V2.0 Metadata Interoperability Profile Version 1.0 [MetaIOP].	Constrained	Cyber-Auth Deployments MUST NOT use this profile
In addition, implementations MUST support the use of the <md:KeyDescriptor> element as follows:	Support	
• 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.	Constrained	No OPTIONAL mechanisms are supported
• 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 behavior of the validation mechanisms they employ, particular with respect to limitations or divergence from PKIX [RFC5280].	Support	Cyber-Auth Deployments MUST follow the requirements specified in Section 2.4.5 Security

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
• 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.	Constrained	Cyber-Auth Deployments MUST follow the requirements specified in Section 2.4.5 Security
• 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.	Constrained	No OPTIONAL additional constraints are supported
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.	n/a	
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.	Support	
2.2.2 Metadata Exchange		

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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).	Constrained	The GC Credential Federation Governance Body maintains and distributes current metadata. To terminate Federation member use of non-current metadata, the GC CFGB stops distributing it. In addition, the GC CFGB may revoke a certificate in the metadata file for reasons including, but not limited to terminating a Federation member's participation, certificate compromise, and key changes. • Federation members MUST submit the XML metadata document to the GC CFGB. • Federation members MUST only accept XML metadata documents from the GC CFGB.
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 behavior unspecified if a single entity's metadata is present in more than one source.	Support	

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
Importation of multiple entities' metadata contained within an <md:EntitiesDescriptor> element MUST be supported.	Support	
Finally, implementations SHOULD allow for the automated updating/reimportation of metadata without service degradation or interruption.	Support	
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 behavior of the validation mechanisms they employ, particular with respect to limitations or divergence from PKIX [RFC5280].	Constrained	• Federation members MUST sign their metadata using the signing certificate issued by the GC ICM Service. • At consumption time, the Federation member relying upon the metadata MUST check the revocation status of the certificate used to sign the metadata. o Only CRL's are supported
2.3 Name Identifiers		

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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	Constrained	Cyber-Auth Deployments MUST support persistent Cyber-AuthDeployments MUST NOT support transient
Support for other formats is OPTIONAL.	Constrained	Cyber-AuthDeployments MUST NOT support other formats
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].	Constrained	Cyber-AuthDeployments MUST follow the requirements specified in Section 2.4.1 Required Assertion Attributes

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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.	Constrained	Cyber-Auth Deployments MUST follow the requirements specified in Section 2.4.1 Required Assertion Attributes
2.5 Browser Single Sign-On		
This section defines an implementation profile of the SAML V2.0 Web Browser SSO Profile [SAML2Prof].	Support	
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].	Constrained	Cyber-Auth Deployments MUST support the Identity Provider Discovery Profile specified in [SAML2 Prof] Cyber-Auth Deployments MUST NOT support the Identity Provider Discovery Service protocol Profile specified in [SAML2 Disco]
2.5.2 Authentication Requests		
2.5.2.1 Binding and Security Requirements		

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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.	Support	
Support for other bindings is OPTIONAL.	Constrained	Cyber-Auth Deployments MUST NOT support other bindings
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):	Constrained	As specified below
• AssertionConsumerServiceURL	Constrained	Cyber-Auth Deployments SHOULD NOT use AssertionConsumerServiceURL • The IDP will obtain this from the metadata
• ProtocolBinding	Constrained	If present, ProtocolBinding attribute MUST be urn:oasis:names:tc:SAML:2.0:bindings: HTTP-POST.

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
• ForceAuthn	Constrained	ForceAuthn MAY be used to require the IDP to force the end user to authenticate to the IDP regardless of the end user's authentication session status at the IDP. • When ForceAuthn is used, the IDP MUST ensure that the principal does not change their NameID from any previous authentication in this session even if it has expired. • if ForceAuthn is used and the authentication is successful, this will reset the IDPs AuthnInstant for this principal.
• IsPassive	Constrained	• IsPassive MAY be used if the SP does not wish for the IDP to take direct control of the end user's browser (i.e., show the end user a page). • If IsPassive is true, the end user MUST be able to authenticate in some passive manner, otherwise the resulting response MUST NOT contain an <Assertion>. • This feature allows the SP to determine whether it should alert the end user that he or she is about to interact with the IDP. An example of a passive situation is: the SP discovers through the common domain cookie that the end user may have an active session at a particular IDP.

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
• AttributeConsumingServiceIndex	Constrained	Cyber-Auth Deployments MUST NOT specify AttributeConsumingServiceIndex.
• <saml2p:RequestedAuthnContext>	Constrained	• The authentication request MUST include <RequestedAuthnContext> • The <RequestedAuthnContext> MUST include a Level of Assurance as specified in [SAML2 Assur]. The GC Cyber-Auth LoA's are defined in Section 2.4.2 GC Cyber-Auth Levels of Assurance. • SPs MUST request a specific level of assurance with the "exact" comparison operator. • The SP MAY request more than one level of assurance in priority order. E.g. this is useful when a level 2 is required but the SP is willing to accept a level 3 if a level 2 is not possible.

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
• <saml2p:NameIDPolicy>	Constrained	• <SPNameQualifier> MUST be present o GCCF IDP Authentication Responses use Persistent Anonymous Identifiers that are shared among the GCCF SPs, To ensure these <NameID>'s contain the <SPNameQualifier> attribute, it MUST be sent on the Authentication Request message. o The GCCF has established the value for the <SPNameQualifier> to be "GCCF1"and • <NameIDPolicy> MAY contain AllowCreate attribute. o In general, AllowCreate will be set to true so that if the end user has never used the selected IDP to access the SP, an end user identifier can be created, and SAML messages can be exchanged between the parties. o However, AllowCreate set to false may be useful if the SP wishes to disable credential registration flows in the user interface at the IDP • If Format is present it MUST be urn:oasis:names:tc:SAML:2.0:nameid-format:persistent.

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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].	Support	
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.	Constrained	Cyber-Auth Deployments MUST only support “exact” for the Comparison attribute.
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 alternatve verification mechanisms.	Constrained	Cyber-Auth Deployments MUST NOT support other means of comparison
2.5.3 Responses		
2.5.3.1 Binding and Security Requirements		

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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.	Constrained	Cyber-Auth Deployments MUST support HTTP POST bindings Cyber-Auth Deployments MUST NOT support HTTP Artifact bindings
Support for other bindings, and for artifact types other than urn:oasis:names:tc:SAML:2.0:artifact-04, is OPTIONAL.	Constrained	Cyber-Auth Deployments MUST NOT support other bindings
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).	Constrained	Cyber-Auth Deployments MUST discard unsolicited <saml2p:Response> messages • No Cyber-Auth use case has been identified which requires these
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].	Support	The GCCFGB defines “acceptability of a response location” to mean the metadata registered <AssertionConsumerServiceURL>

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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.	Constrained	Cyber-Auth Deployments MUST NOT support signing of the <saml2p:Response> element
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.	Constrained	Cyber-Auth Deployments MUST NOT deploy OPTIONAL support
2.5.3.2 Message Content		
The Web Browser SSO Profile allows responses to contain any number of assertions and statements. Identity Provider implementations MUST allow the number of 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.	Constrained	Cyber-Auth Deployments MUST only send <saml2p:Response> messages containing at most a single <saml2:Assertion>

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
Identity Provider implementations MUST support the inclusion of a Consent attribute in <saml2p:Response> messages, and a SessionIndex attribute in <saml2:AuthnStatement> elements.	Support	
Service Provider implementations that provide some form of session semantics MUST support the <saml2:AuthnStatement> element's SessionNotOnOrAfter attribute.	Support	See section 2.2 for constraints on Cyber-Auth IDP deployments
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.	Support	
2.5.4 Artifact Resolution		

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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.	Constrained	Cyber-Auth deployments MUST NOT support the HTTP-Artifact binding
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.	n/a	
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.	n/a	
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.	n/a	

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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.	n/a	
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].	Constrained	Cyber-Auth Deployments MUST NOT support
The implementation requirements defined in section 2.5 for the non-holder-of-key profile apply to implementations of this profile.	n/a	
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 behavior suitable for composition with the Single Sign-On profiles defined in sections 2.5 and 2.6.	Support	Cyber-Auth Deployments MUST support when configured to operate as a Proxying IDP

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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.	Support	Cyber-Auth Deployments MUST support when configured to operate as a Proxying IDP
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.	Support	Cyber-Auth Deployments MUST support when configured to operate as a Proxying IDP
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.	Support	Cyber-Auth Deployments MUST support when configured to operate as a Proxying IDP
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.	Support	Cyber-Auth Deployments MUST support when configured to operate as a Proxying IDP

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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.	Support	Cyber-Auth Deployments MUST support when configured to operate as a Proxying IDP
2.8 Single Logout		
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.	Support	
2.8.1 Logout Requests		
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.	Support	

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
Service Provider implementations MUST support the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for both issuance and reception of <saml2p:LogoutRequest> messages.	Support	
Support for other bindings is OPTIONAL.	Constrained	Cyber-Auth SP deployments MAY support HTTP Redirect bindings for issuance of <saml2p:LogoutRequest> messages No other bindings are supported

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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.	Constrained	Cyber-Auth Deployments MUST follow the requirements specified in Section 2.4.4 Name Identifier Management Protocol A number of GC Departments require notification in the event of a credential revocation. To support this capability, [CATS2 IA&S] adds support for the SAML Name Identifier Management Protocol (and Profile). SPs specify their desire for receiving these messages by adding a <ManageNameIDService> element to their `SPSSODescriptor` in the SP's Metadata. IDPs MUST send a <ManageNameIDRequest> to notify SPs in the event that a credential previously used at the SP has been revoked. IDPs are only required to send these NameID termination messages to SPs for whom they have previously sent assertions for the same principal. The messages are sent on the back-channel and must be sent in a timely manner that is approved by the GCCFGB. To support this IDPs MUST adding a <ManageNameIDService> element to their `IDPSSODescriptor` in the IDP's Metadata. For further details of this interaction will be described in [CA ConOps]. Security

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the <saml2:EncryptedID> element when using the HTTP-Redirect binding.	Support	
2.8.1.2 User Interface Behavior		
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.	Constrained	Cyber-Auth deployments MUST NOT deploy support for user intervention governing the choice of propagating logout to other SPs, or limiting the operation to the Identity Provider. • At all times, a Single Logout Request will generate a global logout for the principal's session.
Service Provider implementations MUST support both user-initiated termination of the local session only and user-initiated Single Logout.	Constrained	Cyber-Auth SP deployments MAY only deploy support for Single Logout (i.e. global logout). • Cyber-Auth IDP deployments MUST propagate the logout without user intervention to all SPs involved in the session and respond to the originating SP.

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
Identity Provider implementations MUST also support the administrative initiation of Single Logout for any active session, subject to appropriate policy.	Support	The Cyber-Auth procedures and rules around the use of "administrative initiation of Single Logout for any active session" will be specified by the GCCFGB.
2.8.2 Logout Responses		
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.	Constrained	• Note: HTTP Redirect bindings for issuance of <saml2p:LogoutResponse> messages are deprecated and SHOULD ONLY be used if the <saml2p:LogoutRequest> message was sent using this binding.
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.	Support	
Support for other bindings is OPTIONAL.	Constrained	Cyber-Auth Deployments MUST NOT deploy OPTIONAL support

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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.	Constrained	Cyber-Auth Deployments MUST NOT deploy OPTIONAL support
3 Conformance Classes		
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.	Support	
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])	Support	This requirement extends to the algorithms used for signing URL-encoded SAML messages as described in section 3.4.4.1 of [SAML-Bindings]

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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])	Support	
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	Support	Algorithms used must be CSEC Approved Cryptographic Algorithms for Electronic Authentication and Authorization Applications as documented in ITSA-11. http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-eng.html (current revision)
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	Support	Algorithms used must be CSEC Approved Cryptographic Algorithms for Electronic Authentication and Authorization Applications as documented in ITSA-11. http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-eng.html (current revision)

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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.)	Support	Algorithms used must be CSEC Approved Cryptographic Algorithms for Electronic Authentication and Authorization Applications as documented in ITSA-11. http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-eng.html (current revision)
Support for other algorithms is OPTIONAL.	Constrained	CA Deployments MUST NOT support other algorithms.
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.	Constrained	See section 2.8 above
3.3 Full		

eGov 2.0	CATS IA&S Support Required	Cyber-Auth Deployment Details
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.	Constrained	• Cyber-Auth deployments MUST NOT be configured to meet section 2.6 • Cyber-Auth deployments MUST be configured to meet section 2.7 when configured to operate as a Proxying IDP
End of table		

2.2 Additional Constraints on the [SAML2 *] specifications

In addition to the constraints imposed by this deployment profile on the eGov 2.0 Profile [eGov 2.0] published by the Kantara Initiative, this Cyber-Auth deployment requirements document also imposes some additional constraints on the underlying SAML 2.0 specifications published by the Security Services Technical Committee (SSTC) of OASIS.

SAML2 *	CATS IA&S Support Required	Cyber-Auth Deployment Details
[SAML2 Core] Section 2.7.2, Line 1061 <SessionNotOnOrAfter>	Constrained	Cyber-Auth IDP deployments SHOULD NOT specify the SessionNotOnOrAfter attribute. This allows the SP to choose its own required duration for its security context. • If a GCCF IDP is unable to configure this value to not be sent, then it must set this value to a high value as determined by the GCCFGB.
[SAML2 Core] Section 3.2.1, Line 1489 <saml:Issuer>	Constrained	SP Authentication Request <saml:Issuer> • MUST be present • MUST be a URL reference within the Cyber-Auth governance domain o The Cyber-Auth procedures to assign these need to be specified.
[SAML2 Core] Section 3.4.1, Line 2017 <saml:Subject>	Constrained	SP Authentication Request <saml:Subject> MUST NOT be included. • no Cyber-Auth use cases require the <saml:Subject> element

SAML2 *	CATS IA&S Support Required	Cyber-Auth Deployment Details
[SAML2 Core] Section 3.4.1, Line 2029 <saml:Conditions>	Constrained	SP Authentication Request <saml:Conditions> MUST NOT be included. • no Cyber-Auth use cases require the <saml:Conditions> element
[SAML2 Core] Section 3.4.1, Line 2068 ProtocolBinding	Constrained	SP Authentication Request ProtocolBinding • MAY be used • If ProtocolBinding is present it MUST be "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
[SAML2 Core] Section 3.6.1, Line 2421 <ManageNameIDRequest>	Constrained	IDP deployments MUST send in a timely manner a <ManageNameIDRequest> with <Terminate> for a credential that has been revoked to any SP that has an endpoint defined for the <ManageNameIDService> and for which it has previously sent an assertion for the principal. IDP deployments MUST NOT send any other <ManageNameIDRequest> messages. SP deployments MUST respond to <ManageNameIDRequest> messages

SAML2 *	CATS IA&S Support Required	Cyber-Auth Deployment Details
[SAML2 Core] Section 8.3.7, Line 3318 Persistent name identifier's <SPNameQualifier>	Constrained	GCCF IDP Authentication Responses use Persistent Anonymous Identifiers that are shared among the GCCF SPs, To meet the [SAML2 Core] requirements, these <NameID>'s must contain the <SPNameQualifier> attribute. • The GCCF has established the value for the <SPNameQualifier> to be "GCCF1"
[SAML2 Bind] Section 3.5.3, Line 785 <RelayState>	Constrained	<RelayState> MAY NOT be included in a response message unless it has been provided in a corresponding request message.
[SAML2 Assur] Section 3, Line 276 <assurance-certification>	Constrained	Metadata for Cyber-Auth IDPs MUST specify the supported Level(s) of Assurance in the <assurance-certification> attribute as defined in [SAML2 Assur], Section 3 Identity Assurance Certification Attribute Profile The URI values to be used for the 4 levels of Assurance are defined in Section 2.4.2 GC Cyber-Auth Levels of Assurance. Multiple LoA values MAY be specified in the IDP's Metadata but only a single value is returned in an authentication response.
[SAML2 Meta] Section 2.3.2, Line 371 <entityID>	Constrained	<entityID> MUST be agreed upon by the entity and the GCCFGB

SAML2 *	CATS IA&S Support Required	Cyber-Auth Deployment Details
[SAML2 Meta] Section 2.3.2.1, Line 443 <Organization>	Constrained	It is RECOMMENDED that <Organization> be present and include either OrganizationName or OrganizationDisplayName.
[SAML2 Meta] Section 2.3.2.2, Line 476 <ContactPerson>	Constrained	<ContactPerson> is RECOMMENDED Cyber-Auth suggests including include either EmailAddress or TelephoneNumber
[SAML2 Meta] Section 2.4.1, Line 550 <RoleDescriptor>	Constrained	• Metadata element <RoleDescriptor> MUST NOT be used
[SAML2 Meta] Section 2.4.3, Line 683 <IDPSSODescriptor> including Section 2.4.2, Line 643 <SSODescriptorType>	Constrained	• WantAuthnRequestsSigned MUST be set to true. • Exactly two instances of <SingleLogoutService> MUST be present (one for each of the Bindings: SOAP and HTTP Redirect) • Exactly one <SingleSignOnService> MUST be present. • Exactly one < ManageNameIDService> MUST be present to receive responses to NameID termination messages. The binding MUST be set to urn:oasis:names:tc:SAML:2.0:bindings:SOAP.

SAML2 *	CATS IA&S Support Required	Cyber-Auth Deployment Details
[SAML2 Meta] Section 2.4.4, Line 736 <SPSSODescriptor> including Section 2.4.2, Line 643 <SSODescriptorType>	Constrained	• AuthnRequestsSigned MUST be set to true. • WantAssertionsSigned MUST be set to true. • <AssertionConsumerService> MUST be included • Exactly one <AssertionConsumerService> MUST have the Binding set to urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST. • Exactly one < ManageNameIDService> MAY be present to communicate the desire to receive NameID termination messages from IDPs. The binding MUST be set to urn:oasis:names:tc:SAML:2.0:bindings:SOAP.
[SAML2 Meta] Section 2.4.5, Line 828 <AuthnAuthorityDescriptor>	Constrained	<AuthnAuthorityDescriptor> MUST NOT be used
[SAML2 Meta] Section 2.4.6, Line 861 <PDPDescriptor>	Constrained	<PDPDescriptor> MUST NOT be used
[SAML2 Meta] Section 2.5, Line 938 <AffiliationDescriptor>	Constrained	<AffiliationDescriptor> MUST NOT be used

SAML2 *	CATS IA&S Support Required	Cyber-Auth Deployment Details
[SAML2 MetaUI] Section 2.1.1 <md:UIInfo>	Support	SP metadata MAY include the elements <mdui:DisplayName> and <mdui:Logo> The IDP MAY use these metadata elements to inform the user about the entity requesting an authentication during the associated authentication dialogue.
End of table		

2.3 Additional Extensions relative to the [SAML2 *] specifications

In addition to the constraints imposed by this deployment profile on the eGov 2.0 Profile [eGov 2.0] published by the Kantara Initiative, this Cyber-Auth deployment requirements document also extends the underlying SAML 2.0 specifications published by the Security Services Technical Committee (SSTC) of OASIS.

SAML2 *	CATS IA&S Support Required	Cyber-Auth Deployment Details
None defined		
End of table		

2.4 Other GC Requirements

In addition to the constraints imposed by this deployment profile on the eGov 2.0 Profile [eGov 2.0] published by the Kantara Initiative, and the additional constraints and extensions on the underlying SAML 2.0 specifications published by the Security Services Technical Committee (SSTC) of OASIS, this Cyber-Auth Deployment Requirements document also imposes some additional requirements for the GC's Cyber-Auth environment.

2.4.1 Required Assertion Attributes

Cyber-Auth Requirement	CATS IA&S Support Required	Cyber-Auth Deployment Details
[SAML2 Core] Section 2.7.3, Line 1165 <AttributeStatement>	Extended	Cyber-Auth SP and IDP Deployments MUST support Cyber-Auth mandatory attributes: • As defined in 2.4.1.1 Mandatory Attributes
[SAML2 Core] Section 2.7.3, Line 1165 <AttributeStatement>	Extended	Cyber-Auth IDP Deployments MAY support Cyber-Auth optional attributes: • As defined in 2.4.1.2 Optional Attributes
[SAML2 Core] Section 2.7.3, Line 1165 <AttributeStatement>	Constrained	Cyber-Auth SP Deployments SHALL NOT support receiving any other attributes • A Cyber-Auth SP Deployment MUST discard any other attributes and not use the attribute values for any processing.
End of table		

2.4.1.1 Mandatory Attributes

Name (URI)	Description	Format	Datatype
ca:gc:cyber-authentication:basic:specVer	The version of the interface specification	MUST be “2.0” for this interface specification [CATS2 IA&S]	xs:string
End of table			

2.4.1.2 Optional Attributes

Name (URI)	Description	Format	Datatype
ca:gc:cyber-authentication:basic:assuranceLevel	Deprecated: only included for transition from version 1 of [CATS1 IA&S] The confidence level of the end authentication mechanism	MUST be one of 1, 2, 3, 4, or test	xs:string
urn:oid: 2.16.840.1.113730.3.1.39	Deprecated: only included for transition from version 1 of [CATS1 IA&S] The end user's preferred language (it is expected that this will be set when the end user changes their language preference during interaction with the IDP)	MUST conform to the definition of the Accept-Language header field defined in [RFC2068] with one exception: the sequence "Accept-Language" ":" # should be omitted.	xs:string
End of table			

2.4.2 GC Cyber-Auth Levels of Assurance

Authentication Requests and Responses for the GC Cyber-Auth credentials will carry the required Level of Assurance. There are 4 Levels of Assurance that are defined in [ITSG-31] and used by the GC Cyber-Auth Program. The URI's representing these LoA's have the following values:

- 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

The schemas corresponding to these values are available from the GC CFGB

2.4.3 Communicating Language Preferences

To meet the GC's Policy requirements, a method was required to send the user's (not the browser's) current language preference from the SP to the IDP and from the IDP to the SP in all cases, even when authentication fails and an assertion is not produced. Cyber-Auth will do this by utilizing a session cookie in a Common Domain defined by the GCCFGB (which may be the same domain established for the IDP Discovery Profile).

This session cookie will carry the language attribute, the values of which are defined in [RFC 1766]. Acceptable values for the Cyber-Auth language attribute include:

- en
- fr

Both SPs and IDPs MUST read this cookie and use this language setting in any user interface pages which are displayed.

Both SPs and IDPs MUST ensure this cookie is set to the user's current language preference prior to issuing a message on an HTTP-Redirect or an HTTP-Post binding. Since it is expected that this GC Language Cookie will be used whether or not the user is within an authentication request/response scenario, it should be updated at the earliest possible time.

Details of the GC Language Cookie in the Common Domain are provided in an annex to this document.

2.4.4 Name Identifier Management Protocol

A number of GC Departments require notification in the event of a credential revocation. To support this capability, [CATS2 IA&S] adds support for the SAML Name Identifier Management Protocol (and Profile).

SPs specify their desire for receiving these messages by adding a <`ManageNameIDService`> element to their `SPSSODescriptor` in the SP's Metadata.

IDPs MUST send a <`ManageNameIDRequest`> to notify SPs in the event that a credential previously used at the SP has been revoked. IDPs are only required to send these NameID termination messages to SPs for whom they have previously sent assertions for the same principal. The messages are sent on the back-channel and must be sent in a timely manner that is approved by the GCCFGB. To support this IDPs MUST adding a <`ManageNameIDService`> element to their `IDPSSODescriptor` in the IDP's Metadata.

For further details of this interaction will be described in [CA ConOps].

2.4.5 Security

To establish trust and secure communications this interface specification relies heavily on X.509v3 cryptographic key pairs. This section outlines the different certificates that are required as well as specifics on their use.

2.4.5.1 The GC ICM Service Certificates

The GC Internal Credential Management Service (GC ICM), operated by PWGSC on behalf of the GC, provides trust and security to the GC Credential Federation. Possession of a valid certificate issued by the GC ICM Service demonstrates membership in the Federation. The GC ICM Service issues three certificates to each SP (one used for TLS, one used for digital signature and one used for encryption), and two certificates to each IDP (one used for TLS and one used for digital signature).

- These certificates MUST be maintained in compliance with the Subscriber responsibilities (as specified by the GC CFGB).

2.4.5.2 Digital Signature

All SAML messages, or parts thereof, MUST be signed by the sender using the GC ICM Service signature certificate that was issued to them. The signature allows the recipient of the message to authenticate the sender, and confirm that the message has not been altered since the time of signature.

- The recipient MUST authenticate the sender and verify the signature upon receipt of the message.
- The recipient MUST verify the revocation status of the sender certificate used to sign the message. Federation member systems MUST use the following method for revocation verification:
    - CRL – the CRL location (in the directory or web site) can be statically configured into the software, and CRL downloaded periodically. See GC ICM documentation (available from GCCFGB) for details regarding distinguished name location and directory hostname.
- If certificate revocation status cannot be determined, the Federation member system MUST reject the message.

2.4.5.3 Encryption

Encryption ensures that only the intended recipient can decipher the message and gain access to confidential information.

- All confidential information in a SAML message MUST be encrypted.
- Encryption MUST use the public key of the intended recipient’s GC ICM-issued encryption certificate.

2.4.5.4 TLS web sites

2.4.5.4.1 For Front-Channel Bindings

This interface specification specifies front-channel bindings using HTTP over TLS (HTTPS) to transport messages.

- Any site managed by a Federation member and using HTTP bindings over TLS MUST secure the TLS session by using a certificate trusted by default by commercially available browsers.
- Use of SSLv3.0/TLS must be compliant with CSE guidelines (e.g., ITSA-11G) and departmental policies.
- HTTPS over TLS (v1.1 or higher) MUST be used unless not supported by the browser
- HTTPS over TLS (v1.0) MAY be used
- HTTPS over SSL (v3.0 or higher) MAY be used only if TLS (v1.0 or higher) is not supported by the browser .
- Earlier versions of SSL MUST NOT be used

2.4.5.4.2 For Back-Channel Bindings

This interface specification specifies back-channel bindings using SOAP over TLS to transport messages.

- Any site managed by a Federation member and using SOAP Bindings over TLS MUST secure the TLS session by using a certificate issued by the GC ICM.
- Use of SSLv3.0/TLS must be compliant with CSE guidelines (e.g., ITSA-11G) and departmental policies.
- TLS (v1.1 or higher) MUST be used
- Earlier versions of TLS or SSL MUST NOT be used

2.4.6 Exception Handling

Cyber-Auth Interface Support Required	Cyber-Auth Deployment Details

Cyber-Auth Interface Support Required	Cyber-Auth Deployment Details
The Cyber-Auth member SAML service MUST handle error conditions gracefully	Specifically, the Cyber-Auth member SAML service MUST handle the list of possible errors provided in 2.4.6.1 “Errors to be handled ”

2.4.6.1 Errors to be handled

The following table lists errors that the Federation member SAML service MUST handle gracefully (i.e. in a controlled user-friendly manner as per the ability of the IDP or SP to respond). This is not a complete list of all possible errors. The table categorizes errors by SAML event.

Error Condition	Cyber-Auth Deployment Requirements
Error Processing <Response> • Incorrect/Unknown <Issuer> • Incorrect Version • Unrecognized InResponseTo • Unacceptable IssueInstant • Status not Success	tbd
Error Processing <Assertion> • Signature Invalid • Signature Certificate Revoked • Cannot determine revocation status • <Assertion> Time Invalid • Cannot Decrypt <Assertion> • Incorrect Recipient • Incorrect Version	tbd

Error Processing <AuthnRequest> • Unknown <Issuer> • Signature Invalid • Signature Certificate Revoked • Cannot determine revocation status	tbd
Error processing SLO Request • Unknown <Issuer> • Signature Invalid • Signature Certificate Revoked • Cannot determine revocation status	tbd
Error processing SLO <Response> • Unknown <Issuer> • Signature Invalid • Unknown status • Signature Certificate Revoked • Cannot determine revocation status	tbd

Appendix A: Additional Functions Beyond Cyber-Auth

A.1. GC Language Cookie

This Appendix defines a method by which an SP or a IDP can discover which language the principal is currently using. This method relies on a cookie that is written in a domain that is common between IDPs and SPs in the GCCF deployment. This domain is established by the GCCFGB and may be the same as the Common Domain used for the IDP Discovery Profile and is known as the <common-domain> in this profile, and the cookie containing the last language in use is known as the GC Language Cookie.

In the GCCF, both SP and IDP entities are required to host web servers in the common domain as defined by the GCCFGB.

A.1.1 GC Language Cookie is in a Common GC Domain

The name of the cookie MUST be "_gc_lang". The format of the cookie value MUST be a single valued text string.

The common domain cookie writing service (see below) SHOULD update the language value whenever the user indicates a different language preference. The intent is that the most recently established language is the one in the cookie. The values of the GC language cookie are defined in [RFC 1766]. Acceptable values for the GC Language Cookie include:

- en
- fr

The cookie MUST be set with a Path prefix of "/". The Domain MUST be set to ".<common-gc-domain>" where <common-gc-domain> is the common gc domain established by the GCCFGB for use with this method (it may also be used with the IDP Discovery Profile). There MUST be a leading period. The cookie MUST be marked as secure.

Cookie syntax should be in accordance with IETF RFC 2965. The cookie MUST be session-only.

A.1.2 Obtaining the GC Language Cookie

Prior to presenting an authentication dialogue to the principal, a IDP MUST know which language the principal desires communication in. To do this, the IDP MUST invoke an exchange designed to present the GC Language Cookie to the IDP after it is read by an HTTP server in the common domain.

The specific means by which the service provider reads the cookie are implementation-specific so long as it is able to cause the user agent to present cookies that have been set with the appropriate parameters. One possible implementation strategy is described as follows and should be considered non-normative. Additionally, it may be sub-optimal for some applications.

- Have previously established a DNS and IP alias for itself in the common domain.
- Redirect the user agent to itself using the DNS alias using a URL specifying "https" as the URL scheme. The structure of the URL is private to the implementation and may include session information needed to identify the user agent.

- Redirect the user agent back to itself.

A.1.3 Setting the GC Language Cookie

Prior to invoking an Authentication Request, an SP MUST ensure the GC Language Cookie is set to the principal's preferred language. Prior to sending an Authentication Response (including error responses), an IDP MUST ensure the GC Language Cookie is set to the principal's preferred language. At any time that the principal chooses to change their language, the SP or the IDP MAY set the GC Language cookie. The means by which the SP or IDP sets the cookie are implementation-specific so long as the cookie is successfully set with the parameters given above. One possible implementation strategy follows and should be considered non-normative. The SP or IDP may:

- Have previously established a DNS and IP alias for itself in the common domain.
- Redirect the user agent to itself using the DNS alias using a URL specifying "https" as the URL scheme. The structure of the URL is private to the implementation and may include session information needed to identify the user agent.
- Set the cookie on the redirected user agent using the parameters specified above.
- Redirect the user agent back to itself.