UNCLASSIFIED

Government of Canada

Identity, Credential and Access Management (GC ICAM) Framework

VERSION 1.1

28 January 2022

GCDOCS#51822376

Revision history

Document version number	Changes	Date
0.1	Initial draft for discussion prepared by TBS-OCIO, Cyber Security	28 September 2021
1.0	Modified to address comments from peer review and incorporated other improvements	6 January 2022
1.1	Incorporated additional changes based on follow up input	28 January 2022

Disclaimer

Any reference to vendors and/or vendor products, implied or otherwise, are for illustrative purposes only and should not be considered an endorsement by the Government of Canada.

Contents

List of Figures

1. Introduction

1.1 Background

Identity, Credential and Access Management (ICAM) is fundamental to a vast majority of the transactions and interactions that occur in support of both internal and external Government of Canada (GC) operations. It is the foundation for trust and confidence between parties exchanging information or permitting access to protected resources. It is a critical enabler of security and privacy and, in the electronic realm, of transactions that can be much more effective and efficient than the legacy methods that they replace. Government business processes need to continue to evolve to leverage the benefits available in new technologies and replace outdated and costly legacy methods.[1]

The scope of ICAM is broad and affects many facets of the business of government. Given its horizontal nature, good ICAM practices need to be pervasive and constantly applied to be effective. Current GC internal ICAM practices are heavily fragmented into silos, both at departmental boundaries and at service and application boundaries, with limited interoperability across these borders. In short, many service providers within the GC have taken on the responsibility and cost of providing these services to their constituency of internal GC workers, with the result that users have far too many credentials to deal with thereby impacting user efficiency, and system owners are bearing the burden of operating their own ICAM systems which, when aggregated across the GC, results in higher costs and reduced security.

The GC is committed to improving its services by providing a more seamless, user-friendly experience while protecting privacy and enhancing security. A trusted GC ICAM system is a key enabler of seamless and frictionless privacy and security in digital systems as it will provide the foundation for stronger access control and accountability, data and service integrity and confidentiality while respecting the rights of users in accordance with Canada's privacy laws. The goal is to realize greater efficiencies and savings for the GC, protect user rights, empower GC workers, and improve the overall integrity of services and capabilities.

For the GC to unlock the full potential of digital identity, it must align to a general set of principles that are technology agnostic and enable an ecosystem that is cost-effective, scalable, trusted, reliable, robust, and user-centric. The GC also has a responsibility to honour applicable policy instruments such as the Policy on Government Security [1] and the Policy on Service and Digital [2] and their associated directives, standards and guidelines. As per the *Directive on Identity Management* [3] the GC is required to:

- manage identity in a manner that mitigates risks to personnel and organizational and national security, while protecting program integrity and enabling trusted citizen-centred service delivery;

[1] It is recognized that the GC will continue to offer services using other methods such as telephone or in-person.

- manage identity consistently and collaboratively within the Government of Canada and with other jurisdictions and industry sectors, where identity of employees, organizations, devices and individuals is required; and
- manage credentials, authenticate users or accept trusted digital identities for the purposes of administering a program or delivering an internal or external service.

A comprehensive, enterprise-wide GC ICAM system based on the framework described in this document is required in order to meet these objectives.

1.2 Purpose/Objective

The purpose of this document is to present the key building blocks of the GC ICAM framework which can be used as a:

- guide to standing up an enterprise-wide ICAM program within the GC;
- tool in creating a road map for service implementation;
- foundation for the development of more detailed ICAM solution architectures;
- tool for governing bodies to assist in evaluating initiatives which are seeking endorsement;
- tool to map existing initiatives in order to identify gaps, redundancies and overlapping initiatives; and
- reference to align to the GC's vision of managing ICAM components.

It should be noted that this framework was heavily influenced by the US Federal Identity, Credential and Access Management (FICAM) [4] program; but expanded and contextualized for the GC. Furthermore, the US FICAM playbook is described using a service-oriented architecture whereas the GC ICAM framework is more aligned with a component-based approach.

1.3 Intended Audience

The intended audience for this document includes, but is not limited to, the GC Enterprise Architecture Review Board (EARB), Departmental Architecture Review Boards (DARB), architects, security practitioners and others who are practicing or interested in the ICAM space within the GC.

1.4 Scope

This documented is intended to describe concepts, processes and technologies from a high-level perspective that can be used as the basis for the development of more detailed solution architectures. The framework applies to both external and internal on-line systems and services supported by the federal government, meaning systems that interact with the public as well as systems that implement internal government processes. Services that are delivered using other methods (such as by telephone or in-person) are not in scope.

While many of the concepts presented in this document may apply to other domains, the scope of this document is limited to Unclassified, Protected A and Protected B environments.

2. Context

2.1 Overview

GC ICAM consists of the policies, procedures, personnel and technology to ensure that access to protected resources is provided only to authorized entities and that the scope of that access is limited to the functions necessary to carry out the responsibilities of that entity. As Gartner defines it, ICAM[2] is the discipline that enables the right individuals to access the right resources at the right times for the right reasons. [5] Within the GC ICAM framework, this extends not only to individuals but also to devices, applications, businesses, and other resource consumers.

To achieve the above outcomes the GC ICAM framework gives a technology and vendor agnostic view of the various layers and components of the digital identity ecosystem which, in turn, support downstream GC services, programs and applications, as represented in Figure 2-1.

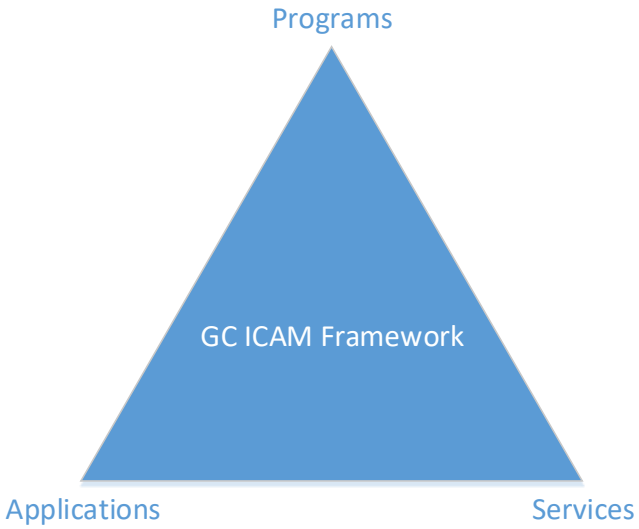


Figure 2-1 GC ICAM Framework in Relation to Services, Applications and Programs

Note that this framework is a sub-component of the overall Enterprise Security Architecture (ESA), which in itself is a subset of the GC enterprise architecture.[3] Figure 2-2 depicts how the GC ICAM framework is situated relative to other OCIO (Office of the Chief Information Officer) architectures.

[2] Gartner actually refers to this as Identity and Access Management (IAM).

[3] See https://www.gcpedia.gc.ca/wiki/Government_of_Canada_Enterprise_Security_Architecture_(ESA)_Program for additional information regarding ESA and https://www.gcpedia.gc.ca/wiki/ICAM for GC ICAM.

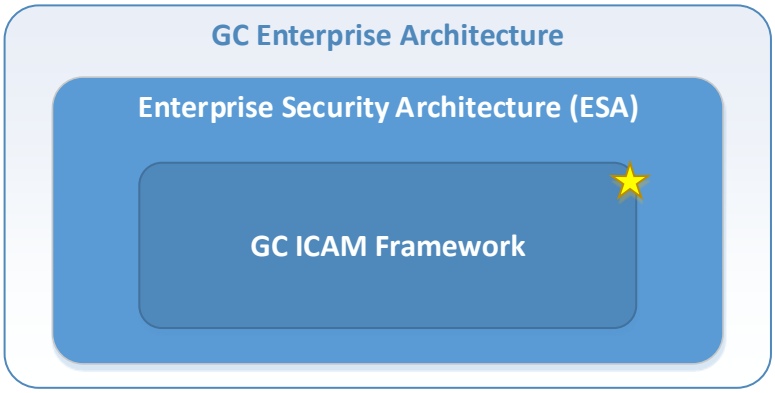


Figure 2-2 GC ICAM Framework Relative to the GC Enterprise Architecture

These building blocks can be referenced and used as a guide to shape a department's own ICAM program and services in alignment with the requirements and objectives outlined in this document. This should make it easier for a department to stand up its own program and ensure it aligns to the broader GC Enterprise Architecture vision. However, where enterprise ICAM services exist, they should be leveraged in accordance with the Policy on Service and Digital [2][4] rather than creating one-off, siloed solutions that typically result in worse user experience, a lowered security posture, and increased costs across the GC. Further, the Chief Information Officer of Canada is responsible for providing direction and defining enterprise-wide requirements for the management of identities, credentials, and access for the Government of Canada and departments[5], while Deputy Heads are responsible for managing departmental approaches for identity assurance and accepting trusted digital identities to support interoperability by using approved trust frameworks[6]. In addition, it should be noted that all implementations of programs, applications and services should respect the GC Digital Standards [6] as outlined in Section 2.3 below.

2.2 Internal versus External

As stated under the Scope section above, the GC ICAM framework addresses both internal and external facing requirements. While the foundational building blocks under the GC ICAM Framework are the same, it is important to recognize that the context is different. For example, how a business manages an employee's identity might be different from how the GC manages the identities of Canadians and residents applying for services. There may be different use cases, different risks, different implications and different goals. Nonetheless, as GC ICAM and supporting technologies evolve, there may be synergies between external and internal domains that can provide greater integration leading to a more seamless user experience.

[4] As per Section 4.4.2.3 of the Policy on Service and Digital [2].
[5] As per Section 4.4.1.10 of the Policy on Service and Digital [2]
[6] As per Section 4.4.2.8 of the Policy on Service and Digital [2]

For internally facing services, the vision is to create and issue a single, strong, and persistent digital identity for GC workers (e.g., employees and contractors) that can be accepted across the enterprise.

Guiding principles that apply to internal entities and capabilities include:

- Enhance the user experience to the maximum extent possible (e.g., reduce the number of credentials required, support SSO, provide consistent and easy to use user interfaces, etc.).
- Leverage existing authoritative sources wherever possible.
- Support multiple authentication options as a one-size fits all approach is unlikely to meet all of the GC's requirements (e.g., credential/authenticator solutions that work well in one environment may not work well in another); however, individual users should not have to be burdened with multiple credentials/authenticators unless absolutely necessary.
- Leverage existing devices wherever possible (e.g., already deployed GC managed smart phones could be used as a second authentication factor) in order to help reduce total cost of ownership (TCO) and minimize the impact on the user experience.
- Base the solutions on open, industry accepted standards, protocols and APIs in order to promote interoperability and avoid vendor lock-in.
- Evolve identity, credential and access management capabilities in support of the Zero Trust security model[7].

Note that a centralized enterprise authentication solution is an essential component in the GC ICAM strategy as it will support many of the principles identified above including reducing the burden on users as well as applications, enabling SSO and facilitating the ability to support multiple authentication methods including MFA.

For externally facing services, the vision is to enable individuals and businesses to use a digital identity of their choice to access GC services with confidence and ease. Guiding principles for external entities include:

- Control and choice for individuals and businesses. Users will be able to access services using an approved credential of their choice to access on-line services.[8]
- Leverage trusted sources of identity from the public sector. Issuance of foundational evidence of identity (e.g., birth certificates, permanent resident cards, articles of incorporation) must continue to lie with the public sector to ensure all individuals obtain foundational credentials and thus should be leveraged to build the digital identity ecosystem.
- Minimal use and retention of identity information to deliver services. The GC will only use and retain as much identity information as necessary. Consent, revocation of consent, and opt-out options are implemented by design and made clear to users.
- Seamless and transparent information sharing where users only need to prove who they are once (i.e., "tell us once"), using their trusted digital identity to access services, under the terms

[7] Refer to the *GC Zero Trust Security Framework* [12] for more information.

[8] This assumes that the credential must be supported by the GC and meet the minimum level of assurance required to access the protected resource.

and conditions they agree to. The GC will be transparent on what client personal information is being collected and for what purpose.

- Use standards based, digital technology and existing processes to streamline services, improve security, and enable greater interoperability while also giving jurisdictions the flexibility to implement solutions that best meet the needs of their respective clients.
- Be capable of evolving and scaling. Digital identity efforts today must also be viable in tomorrow's digital economy, which is poised to grow significantly.

2.3 Mapping to the GC Digital Standards

The guiding principles below build upon the GC Digital Standards [6] with a digital identity lens applied to them.

- **Design with users** by conducting user testing to ensure that everyone is comfortable and confident in using their trusted digital identity to access services.
- **Iterate and improve frequently** leveraging agile methods (e.g., proof of concepts, pilots) to ensure accessing services with trusted digital identities is properly tested on a diverse population before being rolled out to the entire country.
- **Work in the open by default** leveraging approved trust frameworks to disseminate for broader use to the outside world (e.g., private sector).
- **Use open standards and solutions** to facilitate interoperability across devices, platforms, jurisdictions and borders and avoid vendor lock-in.
- **Address security and privacy risks** by using technology and methods of information exchange that minimize unnecessary or unauthorized disclosure of identity information and mitigates the level of security and privacy risks from beginning to end.
- **Build in accessibility from the start** to allow users to see all of their information and control how it is used and shared, as well as ensuring that accessing and receiving government services with a trusted digital identity reflects diverse user needs and will work for everyone.
- **Empower staff to deliver better services** by using innovative tools, methods (e.g., agile), and flexible working arrangements to maintain and retain talent, as well as deliver accelerated digital identity initiatives that reflect value for money.
- **Be good data stewards** by using and retaining only as much identity information as necessary. Consent, revocation of consent, and opt-out options should be implemented by design and made clear to users. In addition, proof of identity validation is recorded, stored in a secure manner.
- **Design ethical services** to ensure fair treatment of all users and respect their rights to privacy as well as comply with ethical design guidelines in the design and use of systems which automate decision making, such as facial recognition or other biometrics.

- **Collaborate widely with multidisciplinary teams** (e.g., IT, communications, policy, privacy, security) to accelerate digital identity initiatives at the enterprise level and deliver value to users.

3. GC ICAM Framework Components

The GC ICAM framework is comprised of a set of core components, ancillary components and supported components as follows:

Core Components

Identity Management	The policies, procedures, processes and technology used to verify and manage digital identities
Credential Management	The issuance, management and revocation/deactivation of credentials and the associated token/authenticator
Access Management	Controlling access to protected resources through appropriate authentication and authorization

Ancillary Components

Federation	Technology, policies, standards, legal agreements and processes that allow organizations to accept and trust digital identities, attributes, and credentials managed by other organizations
Governance	The set of practices and systems that guides ICAM functions, activities, and outcomes
Authoritative Sources	A repository or system that contains identity information about an individual and is considered to be the primary or most reliable source for this information within a given context

Supported Components

Resource Consumers	Entities that require access to Protected Resources
Protected Resources	The applications, services and infrastructure components that Resource Consumers interact with or need access to

These components, and their associated sub-components, work in concert together to form the foundation for the GC ICAM framework as illustrated in Figure 3-1. Note that the dependencies and interactions between these components/subcomponents can be complex and will vary depending on the particular scenario or use case. This level of granularity will be addressed as part of more detailed solution architecture development. Also note that the Level of Assurance (LoA) oval in the diagram is not a separate component in itself. As illustrated, it applies to multiple areas and is discussed in the applicable sections.

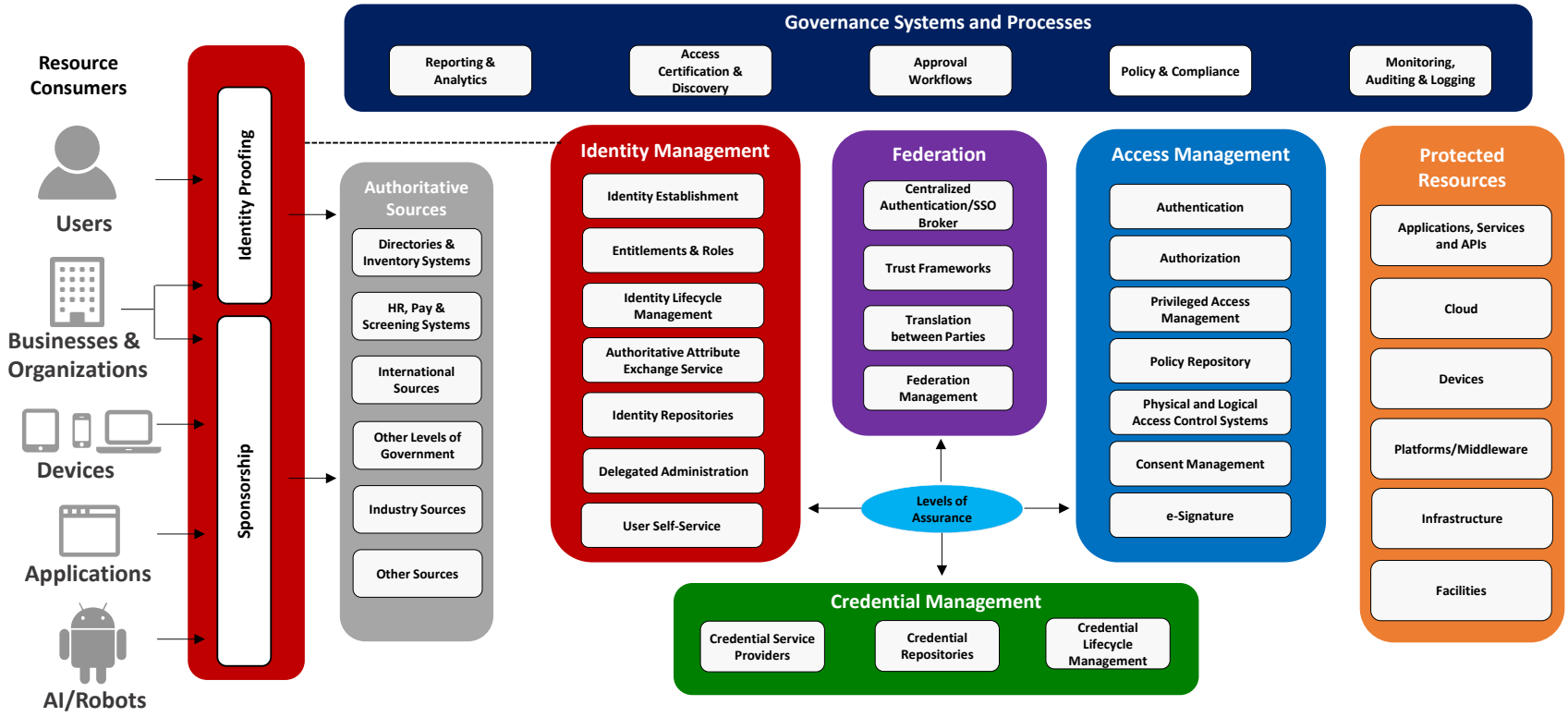


Figure 3-1 GC ICAM Framework Components

Additional details regarding these components/sub-components are provided in the subsections below.

3.1 Core Components (Identity, Credential and Access Management)

3.1.1 Identity Management

Identity management consists of the policies, procedures, processes and technology used to verify and manage digital identities. At its most fundamental level, a digital identity consists of a collection of identity attributes that are managed across the enterprise in support of access control and tailored service delivery. The various subcomponents that comprise identity management are discussed in the subsections that follow.

3.1.1.1 Identity Proofing

Identity is a reference or designation used to distinguish a unique and particular individual, organization, device, application, or any other applicable resource[9]. Identity Proofing is "the function of collecting evidence [identity attributes] which supports a claim of identity [for a specific entity] and the validation and verification of that evidence so as to determine the veracity (or otherwise) of the claim". [7]

The rigor of the Identity Proofing process depends on the Level of Assurance (LoA) required as described in the *Guideline on Identity Assurance* [8]. In some cases, specific identity proofing requirements are identified based on the specific program or service offered (e.g., proof of identity for a passport or a health card are published on-line)[10].

Identity Proofing may be performed centrally on behalf of multiple GC programs and services (e.g., personnel security screening and HR functions) or it may be performed directly by the program or service being accessed (e.g., My Service Canada Account links an otherwise anonymous credential such as GCKey to an individual using a code sent directly to that individual via a reliable delivery method such as physical mail to a pre-registered postal address).

3.1.1.2 Sponsorship

Sponsorship is required to formally establish that an organization or Non-Person Entities (NPE) entity requires access to GC resources. The authorized sponsor becomes responsible for managing the lifecycle of these relationships over time.

3.1.1.3 Identity Establishment

An identity attribute is a property or characteristic associated with an identifiable entity (e.g., an individual, device or business) [11]. A collection or set of identity attributes that is sufficient to distinguish

[9] Expanded definition of "identity" from the *Guideline on Identity Assurance* [8].
[10] See https://www.canada.ca/en/immigration-refugees-citizenship/services/canadian-passports/new-adult-passport/identity-documents.html and https://www.ontario.ca/page/documents-needed-get-health-card.
[11] Expanded definition of "identity attribute" from the *Guideline on Identity Assurance* [8].

one entity from another in a given context is referred to as an identity record (or identity information).[12] The creation of an authoritative record of identity that is relied on by others for subsequent government activities, programs and services is referred to as identity establishment. [8] This set of attributes is sometimes referred to as "core identity attributes". Other identity attribute categories include contact attributes (e.g., address, phone number, email address), authorization attributes (i.e., privileges or entitlements – see Section 3.1.1.4) and auxiliary attributes (e.g., language preference – see Section 3.1.1.9).

Note that identity attributes can be retrieved from one or more Authoritative Sources (see Sections 3.1.1.6 and 3.2.3).

3.1.1.4 Entitlements and Roles

Once a core identity has been established, the set of privileges or entitlements associated with that entity need to be established in order to support informed access control decisions. The privileges may be specified as individual authorization attributes and/or they can be associated with a specific role (e.g., a system administrator is permitted to perform specific functions associated with that role). These authorization attributes may be added to an identity record or may be stored and retrieved separately from one or more Authoritative Sources.

3.1.1.5 Identity Lifecycle Management

Once the various attributes associated with a digital identity have been established, they must be managed over time. Management of the lifecycle of digital identities consists of:

- Provisioning: creation of identity attributes associated with the digital identity.
- Maintenance: maintain accurate and up-to-date attributes in an identity record[13] over its lifecycle.
- De-provisioning: deactivate or remove identity attributes or identity records as required.

3.1.1.6 Authoritative Attribute Exchange Service

The Authoritative Attribute Exchange Service (AAES) serves as a broker between multiple, disparate Authoritative Sources and the consumers of the identity information, thus serving as a consolidated identity repository. As illustrated in Figure 3-2, the AAES is comprised of an Authoritative Attribute Manager which retrieves, correlates and consolidates identity attributes from multiple authoritative sources and an Authoritative Attribute Distributor which provides a single access point for consumers to retrieve the identity attributes. The AAES may be implemented as a virtual directory or it may be implemented as a meta-directory with local identity attribute storage as illustrated in Figure 3-2. The identity attributes may be consumed directly by applications/services; and the AAES can help to populate other downstream identity repositories where required. To allow for flexibility, the identity

[12] Derived from FICAM [4] and the *Guideline on Identity Assurance* [8]
[13] This includes all attributes associated with the entity whether part of the identity record or not.

attribute consumers may obtain their identity attributes from the AAES (Consumer 1), another identity repository (Consumer 2) or both (Consumer 3).

In association with the appropriate workflows, the AAES may also support other functions such as Master Data Management[14] and automated account provisioning/de-provisioning.

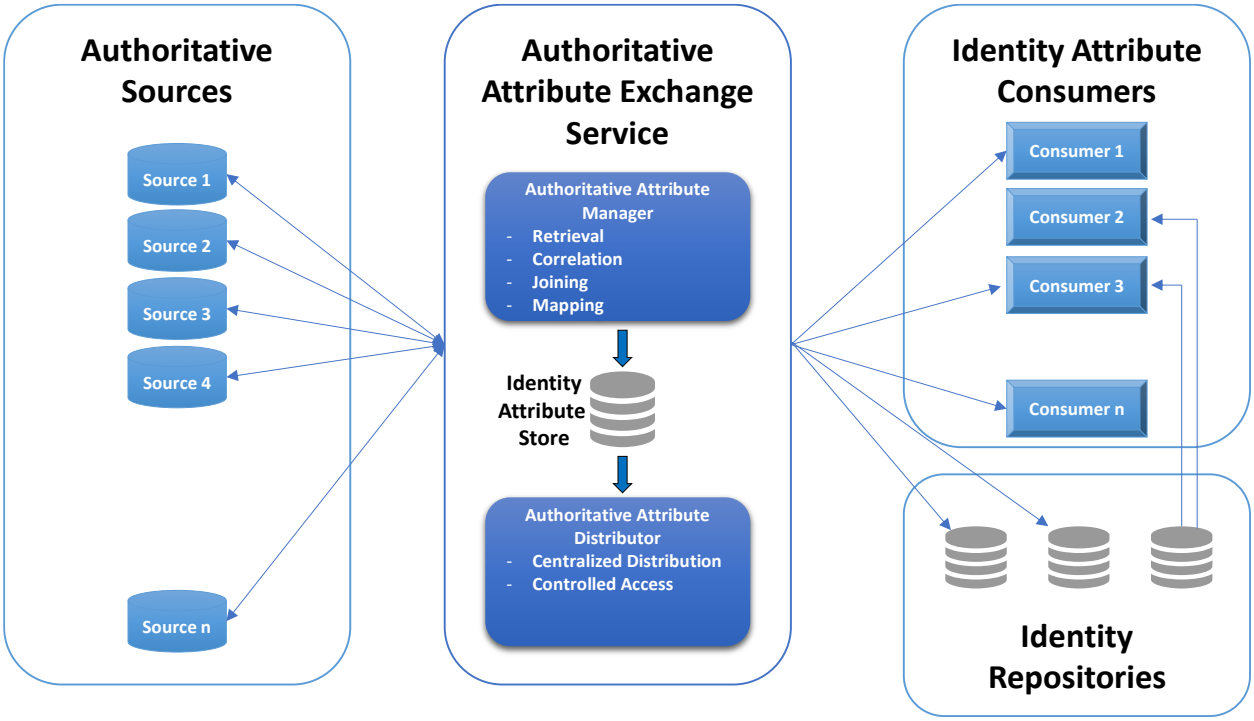


Figure 3-2 - Authoritative Attribute Exchange Service Conceptual Diagram

3.1.1.7 Identity Repositories

Simply put, an identity repository is any data repository that stores identity information. This could be an HR database, a centralized identity attribute store that collects identity information from multiple authoritative sources (as discussed under Section 3.1.1.6 above), or a separate dedicated directory component such as Active Directory.

Figure 3-2 above helps to illustrate the inter-relationships between these various subcomponents. Note that the identity repositories on the right side of the diagram may or may not obtain attributes from the AAES component.

3.1.1.8 Delegated Administration

In the context of IT, delegated administration allows for the de-centralization of certain administrative functions. Essentially, someone in an administrator role (e.g., a system administrator) can assign a subset of less critical administrative functions to someone else, typically someone that is better suited

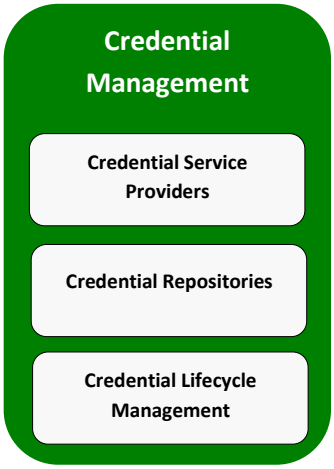
[14] See https://www.gartner.com/en/information-technology/glossary/master-data-management-mdm for Gartner's definition.

to carry out the task(s). For example, an administrator could assign responsibility for managing the profiles of a group of employees to their supervisor. Delegated administration can also be used to facilitate delegation of authority (i.e., a manager with a certain set of authorities could assign a subset or all of those authorities to others). This results in greater efficiencies, reduces the workload on the system administrators, supports business continuity, and is key to scalability in a large organization such as the GC.

3.1.1.9 User Self-Service

In a large enterprise ICAM system, self-service is an important capability to aid in handling scale. For non-authoritative identity attributes such as user preferences (e.g., language preference), a self-service model can meet the requirements without the need to verify the accuracy of the attributes. For authoritative identity attributes (e.g., name, employee id, department) that may be used for access control decisions, a mechanism for confirming correctness of the identity attribute changed via self-service is needed. Self-service also permits users to request new entitlements or roles which are subject to approval by an authorized agent (which may be supported by approval workflows as discussed in Section 3.2.2.3).

3.1.2 Credential Management



In the physical world, credentials can take on many forms including a birth certificate, a driver's license, a passport, a university diploma, a certificate of incorporation, and so on. In the context of the digital world, a credential is an object or data structure that authoritatively binds an entity (e.g., a person, device, organization) to a token or authenticator[15].[16] Both the credential and associated authenticator are used to support the authentication process (see Section 3.1.3.1). Credential management deals with the issuance, ongoing management and revocation/deactivation of credentials and the associated authenticators as discussed in Section 3.1.2.3.

As with identities, credentials are associated with a level of assurance, and target resources will typically have a security requirement that a specific level of credential assurance be used in order to interact with it (e.g., sign in). The four assurance levels associated with credentials are defined in the *Standard on Identity and Credential Assurance* [9] and specific requirements associated with these levels of assurance are provided in *User Authentication Guidance for Information Technology Systems (ITSP.30.031v3)* [10].

As discussed in the *Multi-factor Authentication Considerations and Strategy for GC Enterprise IT Services* [11], the GC must support multiple credential/authenticator types and evolve this support over time as

[15] The term "token" is used in previous versions of NIST SP 800-63 as well as the most recent version of ITSP.30.031 (Version 3). However, NIST changed this term to "authenticator" with the introduction of NIST SP 800-63-3. For the purposes of this GC ICAM framework, the term authenticator is used in keeping with more recent industry trends.

[16] The definition for credential is derived from *User Authentication Guidance for Information Technology Systems (ITSP.30.031v3)* [10]. It is recognized that the distinction between a credential and authenticator is often blurred, but there is a difference between the two. Please consult ITSP.30.031v3 or NIST SP 800-63-3 for additional information.

new requirements and technologies are introduced. This could include password-less authentication based on the FIDO2 standards, use of biometrics to locally authenticate to a device, as well as other emerging technologies such as verifiable credentials.

3.1.2.1 Credential Service Providers

A Credential Service Provider (CSP) is a "trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party, or may issue credentials for its own use."[17] Note that the credential issued by the CSP binds the identity of the subscriber to the associated authenticator. CSPs are responsible for the life cycle management of these credentials/authenticators over time (see Section 3.1.2.3).

For external requirements, the GC currently accepts several different sources of credentials including a number of financial institutions, provincially supplied credentials (currently Alberta and British Columbia only) and a GC branded credential known as GCKey. These credentials are supported by the external GC federation services and users are able to select their preferred credential to access GC on-line services. Although some departments continue to maintain their own legacy credentials, they are encouraged to transition to the GC external federation services wherever possible and all new deployments should include this as a mandatory requirement.

For internal requirements, there are a number of sources that provide credentials including the Internal Credential Management (ICM) Public Key Infrastructure (PKI), departmental PKIs, consolidated SSC and departmental Active Directories, and various other sources including those that are maintained by individual applications/services.

Note that PKI is a fundamental building block of a modern credential architecture. PKI can be used to establish and life cycle manage credentials for both users as well as NPEs such as devices and applications. In addition, PKI can be used to support several security services such as binding an identity to a credential, encryption, digital signatures as well as authentication.

Furthermore, the GC has recently launched an internal federation service referred to as GCpass which is a centralized authentication/SSO broker that will also be capable of issuing credentials to internal users in the future as discussed under Section 3.2.1.1. Any existing or new enterprise applications/services should use the GCpass internal federation service.

3.1.2.2 Credential Repositories

Credential repositories are a fundamental building block of digital identity. Within credential management, they are often holders of primary credentials such as userid/password and are sometimes also a holder of other (secondary) authentication factors. Often credential repositories such as Active Directory also perform the authentication of users against the credentials stored within them. Note that repositories can store credentials, along with other attributes that play an important role in the identity management systems pillar.

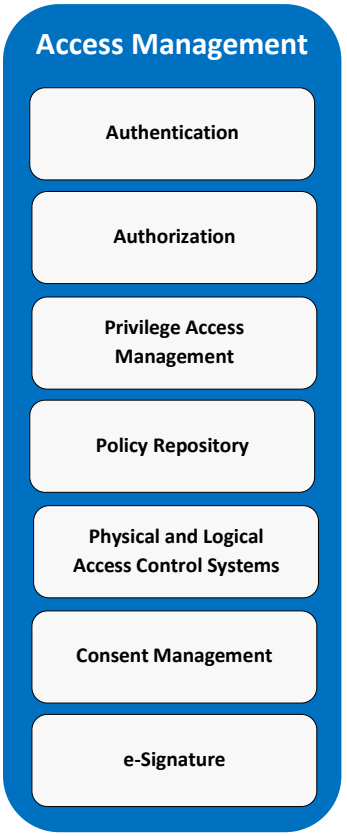
[17] Definition from the NIST SP 800-63-3 and is also consistent with ITSP.30.031v3.

3.1.2.3 Credential Lifecycle Management

Credential lifecycle management (for persons and NPEs) consists of:

- Creation, issuance – creation/activation of one or more credentials which bind the identity of the entity to the associated authenticator(s) and the assignment of those credential(s)/authenticator(s) to a specific entity
- Recovery, reset – to handle loss or compromise of a credential (e.g., a user forgets their password)
- Suspension, blocking, unblocking – temporary deactivation of a credential resulting from extended absence (for example, for long-term personal leave) or suspected compromise of a credential
- Renewal, re-issuance, update – to maintain validity and accuracy of credentials over time
- Revocation, removal, expiry, and destruction – permanent deactivation of a credential due to pre-established expiration, compromise, termination of employment, etc. Depending on the type of credential, it may be re-initialized and re-assigned to another user.

3.1.3 Access Management



Access Management is how an organization authenticates identities and authorizes appropriate access to protected resources [4]. The various components that comprise the Access Management pillar are described below.

3.1.3.1 Authentication

Authentication is verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system [14] or, stated another way, authentication is how the identity of a subject trying to access a resource is verified [4]. In the digital domain, this is done by verifying that the subject attempting to access a resource is in possession of an authenticator that is associated with the subject's credential and that the credential is valid.[18] In the future, other elements may play a role in the authentication process (e.g., user behavioral patterns).

As with identities and credentials, there are four levels of assurance associated with the authentication process as defined in the *Guideline on Defining Authentication Requirements* [15]. Additional information is also provided in *User Authentication Guidance for Information Technology Systems (ITSP.30.031v3)* [10].

Note that authentication is one of several elements that are used to support access control decisions. As the GC moves towards the implementation of a Zero Trust

[18] For example, in a PKI context a subject would activate their PKI authenticator to produce output that is digitally signed with their private key and the subject's public key (extracted from their X.509 public key certificate) is used to verify the authenticator output. In addition, the validity of the subject's credential, which is the X.509 public key certificate in this example, must be assessed which includes making sure the X.509 public key certificate is within its specified validity period and has not been revoked.

security model, access control decisions are expected to be based on multiple considerations such as authentication, entitlements/roles, device status, environmental considerations, behavioral patterns, real-time threat assessment, policy constraints, target resource, etc.

3.1.3.2 Authorization

Authorization is the process of determining whether or not an authenticated entity has permission to access a particular resource. Authorization is typically based on static permissions assigned to the subject or dynamic rules governing the overall system.

Authorization is typically based on one (or more) of four models [4]:

- Access Control Lists (ACLs)
- Role-Based Access Control (RBAC)
- Policy-Based Access Control (PBAC)
- Attribute-Based Access Control (ABAC)

Note that these models are not necessarily mutually exclusive. For example, Gartner recommends a combination of RBAC and ABAC to meet the complex requirements typically associated with implementing authorization solutions [16].

The eXtensible Access Control Markup Language (XACML) specification [17] describes a comprehensive ABAC model that consists of a number of components including Policy Enforcement Points (PEP) which control access to resources (servers, applications, data); and one or more Policy Decision Points (PDP) which render "authorization decisions"[19] based on requests originating from the PEPs. In today's digital service delivery environment, authorization decisions are typically made locally (i.e., each application is responsible for making authorization decisions for their own resources) so the PEP and PDP tend to be co-located in practice. However, the XACML model also makes it possible to centralize authorization decisions[20] in much the same way that authentication is being centralized through federation (see Section 3.2.1) which allows for greater flexibility in the future. In addition, a JSON profile [18] has been defined which provides a simpler, RESTful method for implementing the XACML requests/responses between PEPs and PDPs. Furthermore, the US National Institute of Standards and Technology (NIST) *Zero Trust Architecture* publication (NIST SP 800-207) [19] embraces the XACML model and this is something the GC is investigating as part of its Zero Trust security initiative.

3.1.3.3 Privileged Access Management

Privileged Access Management (PAM) is a specialized area of ICAM that deals specifically with the protection of privileged accounts. Threat actors tend to target privileged user accounts since it gives them access to escalated privileges that non-privileged users do not have. Therefore, additional security controls to protect privileged user accounts are essential in order to help mitigate the risks associated with unauthorized access to accounts with elevated privileges.

[19] The term "authorization decision" is defined and used in the core *XACML specification*.
[20] This is sometimes referred to as "externalized authorization".

According to Gartner[21], PAM consists of the following core capabilities:

- Discovery of privileged accounts across multiple systems, infrastructure and applications
- Credential management for privileged accounts
- Delegation of access to privileged accounts
- Session establishment, management, monitoring and recording for interactive privileged access
- Controlled elevation of commands

Additional considerations include the principle of least privilege, separation of duties, two-person control and just-in-time access.

3.1.3.4 Policy Repository

To provide secure, timely control and access to all resources, accurate, reliable and timely information about resources, users and devices is required. Pairing this information results in the creation of rules/policies that define which attributes a requester must have in order to access a particular resource. The policy repository stores these rules/policies, which, in the simplest cases could be simply access control lists (ACLs) or role assignments for RBAC, but in more complex systems, such as those based on ABAC, consist of dynamically-processed rules for access control.

3.1.3.5 Physical and Logical Access Control Systems

A comprehensive ICAM system must address both logical and physical access control.

A Physical Access Control System (PACS) deals with controlling access to facilities such as an office building as well as restricting access to sensitive areas within a facility such as a room that houses IT assets. Physical access control can be implemented in a variety of ways including building access cards, physical keys, biometrics, voice recognition and/or electronic keypad locks.

A Logical Access Control System (LACS) is "an automated system that controls an individual's ability to access one or more computer system resources such as a workstation, network, application, or database. A logical access control system requires validation of an individual's identity through some mechanism such as a personal identification number (PIN), card, biometric, or other authenticator. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization."[22]

Ideally, PACS and LACS would be fully integrated with shared attributes in order to support security operations that combine physical and logical access. This could include support for geo-gating or the ability to disable both physical and logical access simultaneously.

3.1.3.6 Consent Management

Consent management gives users control over how their personal information is collected, used, retained, and disclosed. It includes user notice, consent, revocation of consent, and opt-out options

[21] Magic Quadrant for Privilege Access Management, 19 July 2021.
[22] Definition provided by the US NIST glossary (see https://csrc.nist.gov/glossary/term/logical_access_control_system)

which are implemented by design and made clear to users. It is guided by compliance to privacy legislation such as the *Privacy Act* [20] and Part I of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) [21][23,24].

In the future, OAuth 2.0 could be used by the GC to support consent management through delegated authorization.

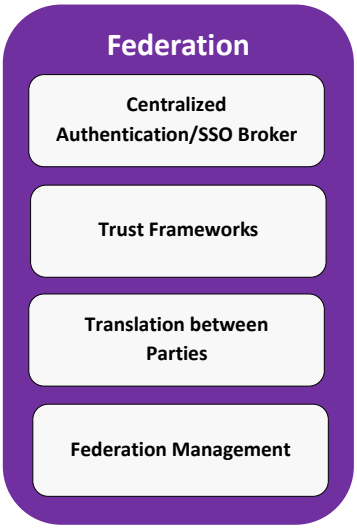
3.1.3.7 Electronic Signature

In support of conducting business electronically, electronic signatures permit users to meet the requirements for a signature in digital form. This can be for many different related purposes such as expressing consent, approval, agreement, acceptance, or authorization of everyday business activities.

Note that e-Signatures can be implemented in a number of ways and at different levels of assurance. Refer to the *Government of Canada Guidance on Using Electronic Signatures* [22] for additional information.

3.2 Ancillary Components (Federation, Governance, Authoritative Sources)

3.2.1 Federation



Federation is the technology, policies, standards, legal agreements and processes that allow one organization to accept and trust digital identities, attributes, and credentials managed by other organizations.[25]

3.2.1.1 Centralized Authentication/SSO Broker

A Centralized Authentication/SSO broker component enables organizations to connect multiple service providers with different identity providers (IdP), while also providing a single sign-on (SSO)[26] capability to end users. This facilitates the trust relationship with identity providers and simplifies how service providers can use existing trusted digital identities, rather than creating their own (the silo problem of identity). This also provides a common user interface which improves and unifies the user experience.

The GC supports external and internal centralized authentication/SSO brokers based on the Security Assertions Markup Language (SAML) and OpenID Connect protocols to enable federation with both

[23] Note that at the time of this writing, new legislation referred to as the Consumer Privacy Protection Act (part of the Digital Charter Implementation Act or Bill C-11) has been proposed to replace Part I of PIPEDA.

[24] Whether explicit consent is required is driven by legislation and there are examples in the public sector where explicit user consent is not required.

[25] Definition is derived from FICAM (see https://playbooks.idmanagement.gov/arch/federation/).

[26] SSO provides access to multiple protected resources based on a single authentication event. This should not be confused with password managers that store multiple passwords that are accessed via a master password. See https://www.canada.ca/en/government/system/digital-government/online-security-privacy/password-guidance.html#toc11 for additional information regarding password managers.

external and internal entities. These protocols support the ability for relying parties to specify the LoAs required for the associated user authentication process. The GC deployment profiles for external federation are available on Github (see https://github.com/canada-ca/CATS-STAE) and the GC deployment profiles for internal federation are available on GCpedia (see GCpass deployment profiles). High-level examples of how these protocols work are provided in Appendix A.

Note that although federation allows credentials issued by a credential provider in one domain to be recognized in other domains, it is important to recognize that it may not always be possible to federate. This could be due to a number of reasons including user choice (e.g., the user does not want to use their existing credentials - such as banking credentials - to access other services), the trust framework in one domain may be incompatible with another domain, the number of domains may become unmanageable, etc. Therefore, it is essential to be able to provide a universal self-serve credential to ensure all users have access to the applications/services they need and the applications/services do not need to manage their own separate credential solutions (also preventing the need for users to re-enroll across multiple applications). To meet internal needs, the universal self-serve credential will be supported by GCpass. GCKey is the universal self-service credential for external users.

3.2.1.2 Trust Frameworks

A trust framework is a set of agreed on principles, definitions, standards, specifications, conformance criteria, and assessment approach [23].

For the GC, the *Public Sector Profile of the Pan-Canadian Trust Framework (PCTF)* [23] and the Canadian Federal PKI Bridge (CFPB) are both foundational trust frameworks that enable interoperability between the GC and partner organizations (such as provinces and territories) across Canada. TBS identity policies such as the *Directive on Identity Management* [3] and the *Guideline on Identity Assurance* [8] as well as the *GC X.509 Public Key Infrastructure Certificate Policy for Person Entity* [24] and the CFPB are foundational for trust within the GC (i.e. between departments).

Note that in certain lower assurance situations, digital identities that do not conform to a GC-approved trust framework may be accepted in order to, for example, improve user experience. Bring your own identity (BYOI) and social media login are examples of this and could be used in situations such as managing lower assurance requirements such as booking a campground site.

3.2.1.3 Translation between Parties

In a federation involving many different organizations sharing digital identity, there is a need to perform certain translation functions to allow the parties to share information appropriately and effectively.

Features of translation include but are not limited to:

- protocol translation – to translate between different protocols (e.g., when one organization uses SAML and the other uses OIDC)
- blinding, pseudonymization, anonymization – to protect privacy of individuals

- attribute translation – to reconcile differences in attribute representations (e.g., when one organization formats names as lastname, firstname and the other as firstname, lastname)

3.2.1.4 Federation (Trust) Management

This is around lifecycle management of trust between federation partners. This would include everything from onboarding new partners to updating policies and maintaining current partner relationships to eliminating expired or non-compliant partners.

3.2.2 Governance Systems and Processes

Governance is the set of practices and systems that guides (e.g., through decision-making, measuring, certification, and policy generation) ICAM functions, activities, and outcomes.[27]

3.2.2.1 Reporting and Analytics

Reporting is "the process of organizing data into informational summaries in order to monitor how different ICAM components are performing and complying with policy". Analytics is "the process of exploring data and reports in order to extract meaningful insights, which can be used to better understand the overall system and improve efficiency [25]."

Reporting and analytics span across many (if not all) ICAM systems including (but not limited to): application layer, data layer, presentation layer, as well as physical systems which interact with the ICAM components.

Examples of reporting and analytics are:

- Application/Platform Certification (Attestation)
- Data/File Access Certification (Attestation)
- Exception Reporting
- Activity-Based Reporting
- Role Certification (Attestation)

3.2.2.2 Access Certification & Discovery

Access certification and discovery is the process of validating access rights within systems. This process is necessary for security risk management and effective governance. With access certification, organizations and regulations aim to formally validate users within systems and ensure their access rights are appropriate [26].

[27] Definition is derived from FICAM (see https://playbooks.idmanagement.gov/arch/governance/)

3.2.2.3 Approval Workflows

Approval workflows are used to manage the life cycle of a digital identity including provisioning, on-going maintenance and de-provisioning of identity attributes (e.g., name, privileges, roles). There can be, and typically are, more than one approval authority depending on the context. In addition, a single approval workflow can require multiple checks from a variety of stakeholders.[28]

Approval workflows could:

- Be triggered automatically, for example when onboarding a new employee
- Arise by user self-service request for access to a resource that requires separate approval
- Be directly configured by an authorized authority (e.g., manager adding team members to a group).

3.2.2.4 Policy & Compliance

Policy and compliance ensures adherence to the organization's policies and applicable laws. This enforcement can be done through a combination of automated and manual processes. Compliance can be further enhanced/evolved through mechanisms that are very formal, such as audits, to informal, such as peer reviews, which can happen on a periodic basis. Certain systems can have specific auditing requirements in order to maintain recognition/certification.

Types of policies could include:

- Privacy
- Security
- HR

Policy and compliance includes remediation of any policy violations.

3.2.2.5 Monitoring, Auditing, and Logging

An audit log is a chronological record of system activities, including records of system accesses and operations performed in a given period [27]. Audit logs provide a record of important events that a given system (or collection of systems) has performed. This can be used to construct an audit trail to examine the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction [27] to facilitate formal audits. Refer to GC Event Logging Guidance [28] for further information.

Monitoring is an umbrella term that can include many facets of system evaluation. This is the process of collecting, aggregating and analyzing metrics to better evaluate the use of the system.

These components work together to ensure the system is healthy, running efficiently and are critical for detection and prevention of anomalies and threats.

[28]Definition is partially derived from https://kissflow.com/workflow/create-approval-workflow-in-less-than-15-min/ [30]

3.2.3 Authoritative Sources

For the purposes of this framework, an authoritative source is a repository or system that contains identity information about an entity and is considered to be the primary or most reliable source for this information within a given context.[29] Typically, authoritative sources are determined by a policy decision of the responsible authority. Ideally, an issuing source[30] would also be an authoritative source but this is not always possible. Note that authoritative sources will need to reflect changes to identity information over time to ensure it remains accurate.

Essentially, these authoritative sources serve as repositories for authoritative identity attributes that can be retrieved and used to support identity, credential and access management functions including linking a credential to an identity, privilege management and tailored service delivery. (Related information regarding attribute exchange is provided under Section 3.1.1.6.)

It should be noted that not all information maintained by these systems is necessarily authoritative (e.g., certain information may not be updated in the amount of time required to meet identity management requirements). In addition, some of these sources may be unwilling or unable to participate for a variety of reasons including privacy concerns or lack of technology to support the necessary functionality. Availability may also be an issue as some authoritative sources may not always be on-line.

3.2.3.1 Directories & Inventory Systems

Directories are a common mechanism for storing information about users and NPEs. Directories have the advantage of being widely accessible and can be used to publish authoritative attributes from other sources and can also be the authoritative source for certain attributes such as credentials and certain identity attributes.

Inventory systems keep track of which components are valid for certain purposes. For example, an inventory of all an organization's devices should be part of a Zero Trust architecture, so that it is possible to restrict access only to devices that have been suitably approved and are known to the organization.

3.2.3.2 HR, Pay & Screening Systems

These are foundational sources of GC user attributes which can be used to make access control decisions and possibly also identity-proofing decisions. Examples of authoritative attributes may include the name of an employee from an HR system, the name of a contractor from a finance system, or security clearance level of an individual from a personnel security screening database.

[29] Note that there is no universally agreed definition for authoritative source. This definition is derived from the definition of "authoritative data source" from the US Department of Energy Order DOE O 206.2 [32] .

[30] The issuing source is the definitive originator of the identity attributes. For example, birth certificates are foundational sources of evidence issued by a province to Canadian born citizens.

3.2.3.3 International Sources

Identity information on non-citizens will need to come from trusted non-Canadian sources. GC organizations have relationships with foreign entities and need trusted sources for identity information before allowing access to GC resources. Examples of trusted international sources might be passports from trusted partner nations and attestations from trusted foreign organizations (e.g., in the defence or law enforcement realm).

3.2.3.4 Other Levels of Government

The GC interacts with various levels of government ranging from provinces and territories to municipalities, including, for example, law enforcement, health care, and judicial. Provinces and territories play a critical role in foundational identity by operating the vital statistics organizations that record all life events (e.g., births, deaths, marriage, name change) as well as information about business (e.g., articles of incorporation, permits, licenses) in their jurisdiction. In addition, a number of GC departments (e.g., RCMP, Health Canada) need to share access to GC data with other levels of government, thus requiring authentication of users and trusted access control decisions that rely on authoritative sources from other levels of government.

User experience and security can be enhanced by leveraging already-established trusted digital identities from other levels of government.

3.2.3.5 Industry Sources

The GC interacts with many industry partners for exchanging information or giving access to GC resources. Businesses are the authoritative source for information about their business, such as business name, area of business, and employee information.

Industry also has identity information collected about their customers (e.g., financial institutions, insurance companies, telecom providers), which can potentially be used (with user consent) as part of identity-proofing or authenticating users accessing GC systems. However, it should be noted that industry identity sources may not always be as strong as foundational government sources, but nevertheless could be used as supporting sources to augment cases where the government sources are not sufficient.

3.2.3.6 Other Sources

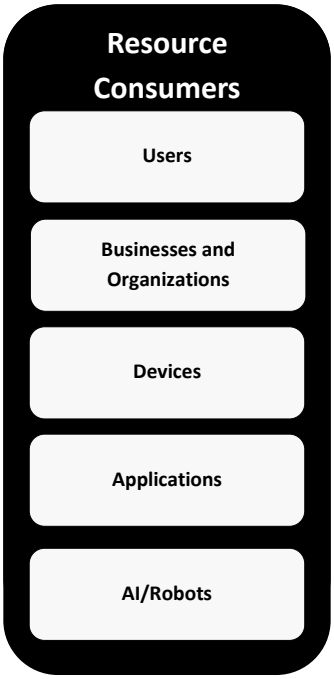
There are many other identity sources that may play a role in providing identity attributes. Some examples are:

- Learning management systems, which are a source of proof of educational credential that may be a pre-requisite to access a certain resource or do a certain job.
- Behavioural, possibly AI-based, systems which keep track of a user's typical patterns of usage and behaviour to identify anomalous access patterns that may be associated with an imposter.
- Privileged access management repositories
- Social media or crowd-sourced identity (likely weak level of assurance)

- Entitlements and policy rules repositories
- Activity logs
- Risk-based rules repositories
- Attributes stored in PKI certificates (likely high level of assurance)
- Platform-specific repositories (e.g., OS/400)

3.3 Supported Components (Resource Consumers, Protected Resources)

3.3.1 Resource Consumers



Resource Consumers are entities that require access to Protected Resources. The Resource Consumers represented in this framework are both internal and external to government. The primary Resource Consumers involved in the GC ICAM ecosystem are described in the subsections below.

3.3.1.1 Users

This includes

- internal users such as:
  - public servants, contractors, RCMP officers, Canadian Forces members, locally-engaged staff (e.g., embassy staff), trusted guests (e.g., interchanges from other governments)
- external users such as:
  - members of the public, visitors, members of other levels of government, and members of businesses and other organizations

Users may be acting on their own behalf or as a proxy for others. A user may also have many roles or personas in their interactions with the GC.

3.3.1.2 Businesses & Organizations

This includes the commercial businesses, non-profit organizations, Indigenous self-government and all levels of government that would need to interact with the federal government for some purpose.

3.3.1.3 Devices

This includes any device that needs to be authenticated to gain access to some resource, such as:

- Mobile devices (including tablets)
- Laptops and desktop computers
- Internet of Things (IoT) / smart devices
- Network devices
- Servers
- Voice assistants

Devices used to access internal GC resources will typically be owned/managed by the GC and will be authenticated (e.g., using device certificates) and assessed before access to internal GC resources is permitted. However, there may be exceptions to this to accommodate certain situations such as consultants (e.g., permitting the use of an unmanaged phone as a second factor for authentication purposes) or allow employees to use their personal devices to access less critical (lower assurance) applications/services such as on-line training. On the other hand, the GC has no control over the devices used by the public to access external facing GC services.

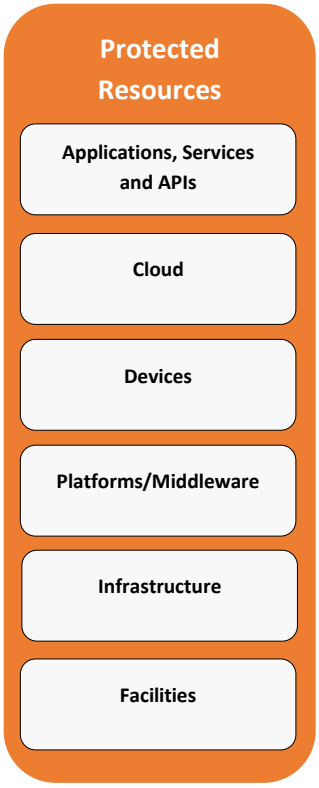
3.3.1.4 Applications

This includes any application that needs to be authenticated in order to interact with another application or service.

3.3.1.5 AI/Robots

Artificial Intelligence (AI) and robots are emerging technologies that are already influencing digital service delivery and are expected to play a significant role in the future. AI/robots can be implemented in various forms including as autonomous entities, acting on behalf of a user (and therefore appear to be that user), or embedded in a device or application.

3.3.2 Protected Resources



Protected Resources are the applications, services and infrastructure components that Resource Consumers interact with or need access to. Protected Resources are the primary reason that ICAM is required (i.e., in order to make appropriate access control decisions).

Note that some Protected Resources (e.g., device and application) appear also as a Resource Consumer in this framework. This is to recognize the fact that non-person entities (NPEs) also interact with other NPEs and must therefore authenticate to one another.

Protected Resources can leverage an enterprise or shared digital identity infrastructure or can implement it themselves, with significant negative consequences for user experience, security, and privacy across the enterprise. An important goal to strive for is to leverage SSO across as many Protected Resources as possible to improve user experience and security.

While not meant to be exhaustive, many of the Protected Resources typically encountered in practice are addressed in the subsections that follow.

3.3.2.1 Applications, Services and APIs

Applications and services take many forms such as portals, enterprise business apps, mobile apps, collaboration apps, on-line services, workloads, etc. Applications usually help facilitate either access to a service or be the service themselves.

Applications and services are built on a wide range of modern and legacy technologies and platforms, which can pose a challenge to an ICAM infrastructure to support effectively.

In more modern systems, Application Programming Interfaces (APIs) are the norm for passing information between systems. The GC will have its own API store to be accessed by other departments and the public, and the GC will also access external information from public APIs provided by other organizations. In order to access GC APIs, users and applications will often need to authenticate and be authorized to view or modify data available over the API using secure mechanisms.

Cloud providers also use ICAM APIs for securely controlling access to services. With these, you can centrally manage users, security credentials such as access keys, and permissions that control which resources users and applications can access [29].

3.3.2.2 Cloud

Although cloud is really just a different way of providing resources and services to a department, it also introduces new mechanisms for administrative (privileged access) control and extensive new ICAM componentry for user authentication and authorization (referred to as IDaaS). In particular cloud introduces its own (sometimes proprietary) directories which may need to interoperate with on premise directories and those from other cloud service providers.

There are also the many different flavours of cloud, such as SaaS, PaaS, and IaaS, as well as public vs hybrid vs private cloud that impact on the ICAM options available.

3.3.2.3 Devices

As with applications, devices take many forms including desktops, laptops, tablets, cell phones, voice assistants and IoT (e.g., scanners, surveillance cameras, electronic sensors). These are managed devices where the GC controls authentication and authorization of their use. Mechanisms for authentication vary and can include passwords, PINs, biometrics (e.g., face or fingerprint) as well as MFA. In the best cases a TPM (trusted platform module) is available on the device to allow it to relay the user authentication that was performed to the device to other endpoints.

Devices come in many flavours of operating system, capabilities, versions, so obtaining a consistent level of ICAM security across many disparate devices can be a challenge.

3.3.2.4 Platforms/Middleware

A platform (or computing platform) is the combination of the operating system and the computer (particularly the CPU) that it runs on. Middleware is software that acts as a bridge between an operating system or database and applications, especially on a network.[31] As Gartner defines it, middleware is the software "glue" that helps programs and databases (which may be on different computers) work together. Its most basic function is to enable communication between different pieces of software.[32]

[31] Definition from Google's English dictionary provided by Oxford Languages.
[32] Definition from Gartner's Glossary (see https://www.gartner.com/en/information-technology/glossary/middleware).

Examples include container orchestration, serverless, virtualization, enterprise service bus, API gateway, devops orchestration, etc.

3.3.2.5 Infrastructure

Infrastructure is a broad category that includes a wide range of technology components including:

- servers (e.g., databases, proxies, storage/backup, domain controllers, jump servers)
- appliances (e.g., black-box devices, virtual appliances, storage, compute, high performance computing)
- network components (e.g., routers, switches, firewalls, access points)
- data centre (e.g., HVAC systems, power management, physical security systems)

Infrastructure components need to be identified, catalogued and issued credentials as necessary to support authentication between (and with) these components.

3.3.2.6 Facilities

Facilities or physical access control systems (PACS) also require the full suite of ICAM functions to make access control decisions. On the other hand, the physical components that make up a PACS are completely different than those that make up a logical access control system (LACS), so interoperability between PACS and LACS is an important consideration in achieving a single, cohesive ICAM solution for the GC. In particular, the authoritative sources, identity management systems, and credential management systems must be interoperable across LACS and PACS.

4. Conclusion

This document describes the key building blocks of the GC ICAM framework. It establishes a common lexicon that can be used to describe individual components that comprise the framework. The framework described in this document will be used to help establish an enterprise-wide approach to ICAM within the GC. It can also be used as a guide to help departments define their own ICAM architecture or determine where there existing ICAM deployments may be improved by addressing gaps or deviations from this framework.

In summary, the objectives of this document are to provide:

- a guide to deploying an enterprise-wide ICAM program within the GC;
- a tool that can be used to create a road map for service implementation;
- a foundation for more detailed/granular ICAM reference/solution architectures;
- a tool for governing bodies to assist in evaluating initiatives which are seeking endorsement;
- a tool to map existing initiatives in order to identify gaps, redundancies and overlapping initiatives; and
- a reference to align to the GC's vision of managing ICAM components.

5. References

[1] Treasury Board of Canada Secretariat, "Policy on Government Security," 2019. [Online]. Available: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578.

[2] Treasury Board of Canada Secretariat, "Policy on Service and Digital," 2020. [Online]. Available: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603.

[3] Treasury Board of Canada Secretariat, "Directive on Identity Management," [Online]. Available: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577.

[4] US Government, "Federal ICAM Architecture," [Online]. Available: https://playbooks.idmanagement.gov/arch/.

[5] Gartner, "Gartner Glossary," [Online]. Available: https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam.

[6] Treasury Board of Canada Secretariat, "Government of Canada Digital Standards," [Online]. Available: https://www.canada.ca/en/government/system/digital-government/government-canada-digital-standards.html.

[7] Kantara, "IAF-1050 Glossary and Overview," [Online]. Available: https://kantarainitiative.org/download/iaf-1050-glossary-and-overview/.

[8] Treasury Board of Canada Secretariat, "Guideline on Identity Assurance," [Online]. Available: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678.

[9] Treasury Board of Canada Secretariat, "Standard on Identity and Credential Assurance," [Online]. Available: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32612.

[10] Canadian Centre for Cyber Security, "User Authentication Guidance for Information Technology Systems (ITSP.30.031v3))," [Online]. Available: https://cyber.gc.ca/.

[11] Treasury Board of Canada Secretariat, "Multi-factor Authentication Considerations and Strategy for GC Enterprise IT Services," [Online]. Available: https://www.gcpedia.gc.ca/gcwiki/images/9/9e/GC_MFA_Strategy.pdf.

[12] Treasury Board of Canada Secretariat, "GC Zero Trust Security Framework," 2021. [Online]. Available: https://www.gcpedia.gc.ca/gcwiki/images/f/fa/GC_Zero_Trust_Security_Framework.pdf.

[13] W3C, "Verifiable Credentials Data Model v1.1," [Online]. Available: https://www.w3.org/TR/vc-data-model/#dfn-credential.

[14] National Institute of Standards and Technology, "Annex A of FIPS 200," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

[15] Treasury Board of Canada Secretariat, "Guideline on Defining Authentication Requirements," [Online]. Available: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262.

[16] Gartner, "A Systematic and Practical Approach to Optimizing Authorization Architecture," 2015.

[17] OASIS, "eXtensible Access Control Markup Language (XACML) Version 3.0," [Online]. Available: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

[18] OASIS, "JSON Profile of XACML 3.0 Version 1.0," 12 October 2017. [Online]. Available: http://docs.oasis-open.org/xacml/xacml-json-http/v1.0/xacml-json-http-v1.0.html.

[19] US National Institute of Standards and Technology, "Zero Trust Architecture (NIST SP 800-207)," [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-207/final.

[20] Government of Canada, "Privacy Act," [Online]. Available: https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html.

[21] Government of Canada, "Personal Information Protection and Electronic Documents Act," [Online]. Available: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html.

[22] Treasury Board of Canada Secretariat, "Government of Canada Guidance on Using Electronic Signatures," [Online]. Available: https://www.canada.ca/en/government/system/digital-government/online-security-privacy/government-canada-guidance-using-electronic-signatures.html.

[23] Treasury Board of Canada Secretariat, "Public Sector Profile of the Pan-Canadian Trust Framework," Version 1.3, [Online]. Available: https://canada-ca.github.io/PCTF-CCP/Version1_3/PSP-PCTF-V-1-3-Consolidated-Overview-EN-2021-04-21.pdf.

[24] Government of Canada, "GC X.509 Public Key Infrastructure Certificate Policy for Person Entity," [Online]. Available: https://www.gcpedia.gc.ca/gcwiki/images/0/07/GC_PKI_Certificate_Policy_for_Person_Entity.pdf.

[25] Adobe, "Reporting vs. Analysis: What's the Difference?," [Online]. Available: https://blog.adobe.com/en/publish/2010/10/19/reporting-vs-analysis-whats-the-difference.html#gs.ay14qj.

[26] Identity Management Institute, "Access Certification," [Online]. Available: https://identitymanagementinstitute.org/access-certification/.

[27] National Institute of Standards and Technology, "SP 800-53 Revision 5, Security and Privacy Controls," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[28] Treasury Board of Canada Secretariat, "Event Logging Guidance," 2020. [Online]. Available: https://www.canada.ca/en/government/system/digital-government/online-security-privacy/event-logging-guidance.html.

[29] Amazon Web Services, "IAM API Reference," [Online]. Available: https://docs.aws.amazon.com/IAM/latest/APIReference/welcome.html.

[30] Kissflow, "How to Create an Approval Workflow in Less Than 15 Min," [Online]. Available: https://kissflow.com/workflow/create-approval-workflow-in-less-than-15-min/.

[31] National Institute of Standards and Technology, "SP 800-63-3 Digital Identity Guidelines," [Online]. Available: https://doi.org/10.6028/NIST.SP.800-63-3.

[32] US Department of Energy, 2013. [Online]. Available: https://www.directives.doe.gov/directives-documents/200-series/0206.2-BOrder/@@images/file.

1

2

3

6. Appendix A – High-level Federation Protocol Examples

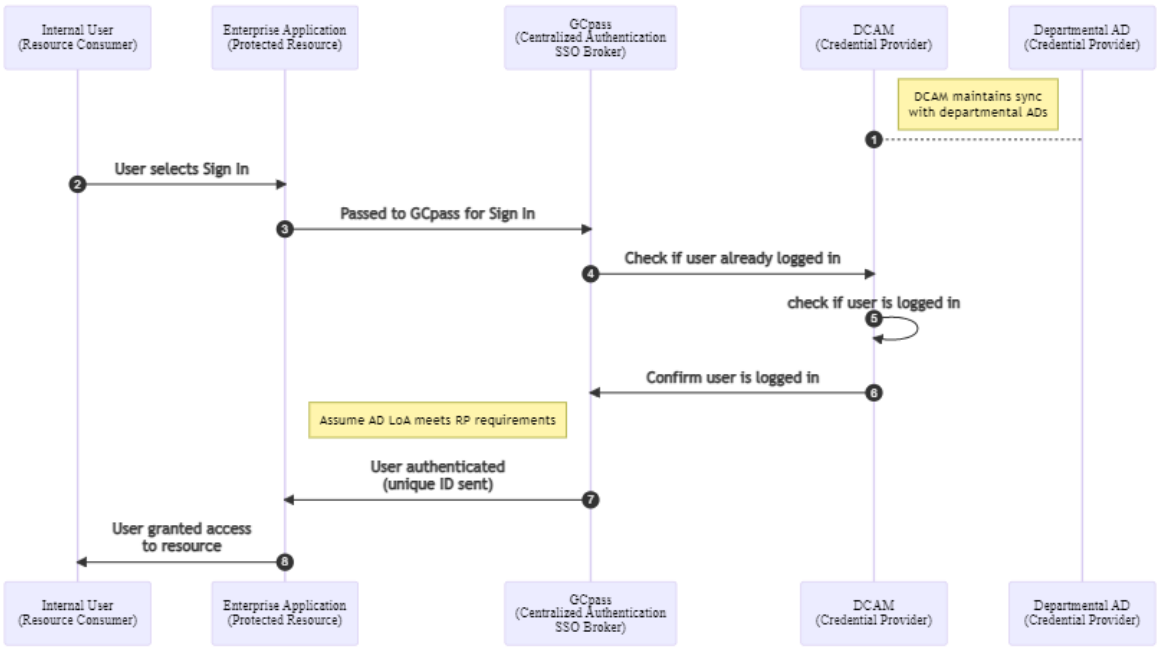


Figure A-1: Internal Use Case

Figure A-1 represents a use case where an internal user (Resource Consumer) is requesting access to a GC enterprise application or service (Protected Resource) after they have logged in through their departmental Active Directory (AD). In this use case, GCpass is the Centralized Authentication/SSO broker and the user's departmental AD is the Credential Provider (coordinated via SSC's DCAM). This use case illustrates the SSO capability supported by GCpass.

Note that the message exchanges between components assume a specific type of protocol binding or flow (in this case a SAML 2.0 redirect binding) – other bindings or flows such as the OpenID Connect 1.0 authorization code flow are also supported. In addition, other credential providers can be supported as discussed in Section 3.1.2.1.

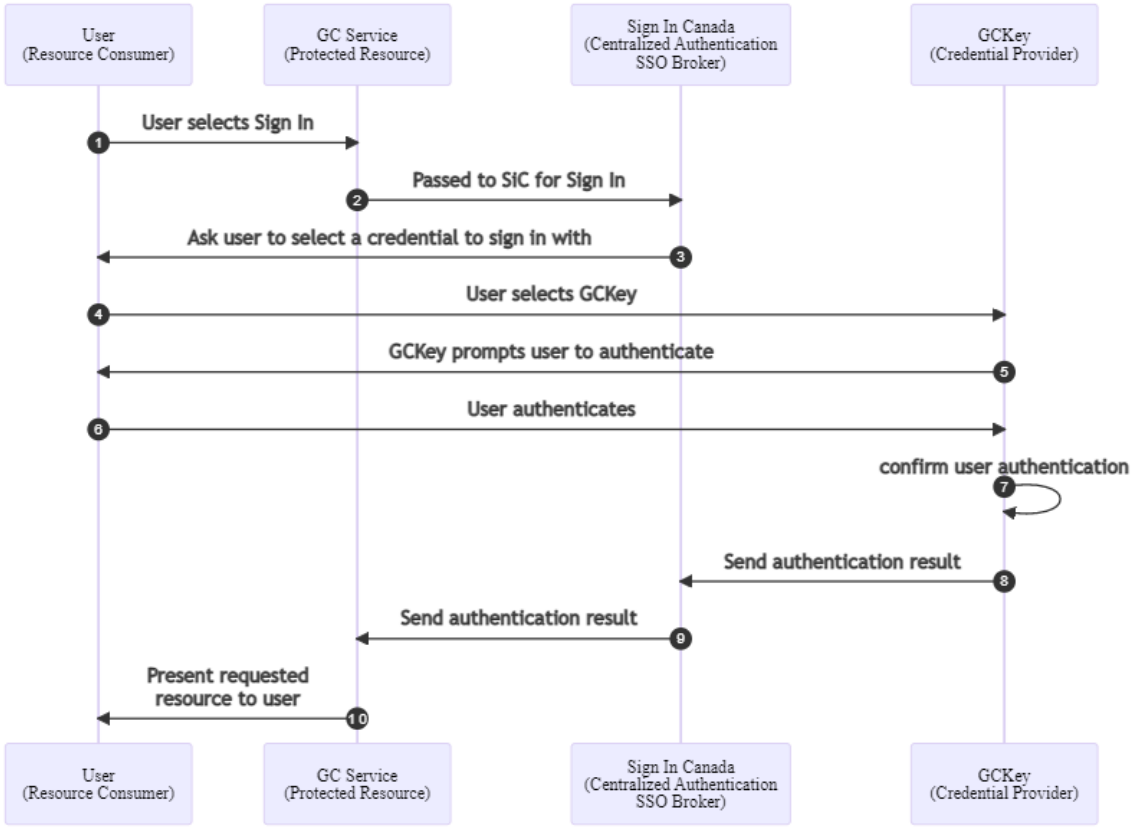


Figure A-2: External Use Case

Figure A-2 represents a use case where an external user (the Resource Consumer) is requesting access to a GC on-line service (the Protected Resource) and the user is not currently logged in. In this use case, Sign In Canada is the Centralized Authentication/SSO broker and GCKey is the Credential Provider.

As with the previous example, the message exchanges between components assume a specific type of protocol binding or flow and exchanges other than those represented are possible. In addition, Credential Providers other than GCKey are also supported as discussed in Section 3.1.2.1.