Identity in the Cloud Use Cases Version 1.0

Committee Note 01

08 May 2012

This is a Non-Standards Track Work Product. The patent provisions of the OASIS IPR Policy do not apply.

Specification URIs

This version:

http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/cn01/IDCloud-usecases-v1.0-cn01.pdf (Authoritative)
http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/cn01/IDCloud-usecases-v1.0-cn01.html
http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/cn01/IDCloud-usecases-v1.0-cn01.doc

Previous version:

http://www.oasis-open.org/committees/download.php/45281/id-cloud-usecases-v1.0-cnprd01.zip

Latest version:

http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/IDCloud-usecases-v1.0.pdf (Authoritative)
http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/IDCloud-usecases-v1.0.html
http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/IDCloud-usecases-v1.0.doc

Technical Committee:

OASIS Identity in the Cloud TC

Chairs:

Anil Saldhana (anil.saldhana@redhat.com), Red Hat, Inc.
Anthony Nadalin (tonynad@microsoft.com), Microsoft

Editor:

Matt Rutkowski (mrutkows@us.ibm.com), IBM

Abstract:

This document is intended to provide a set of representative use cases that examine the requirements on identity management functions as they are applied to cloud based interactions using commonly defined cloud deployment and service models. These use cases are intended to be used

for further analysis to determine if functional gaps exist in current identity management standards that additional open standards activities could address.

Status:

This document was last revised or approved by the OASIS Identity in the Cloud TC on the above date. The level of approval is also listed above. Check the “Latest version” location noted above for possible later revisions of this document.

Technical Committee members should send comments on this document to the Technical Committee’s email list. Others should send comments to the Technical Committee by using the “Send A Comment” button on the Technical Committee’s web page at http://www.oasis-open.org/committees/id-cloud/.

Citation format:

When referencing this document the following citation format should be used:

[IDCloud-Usecases]

Identity in the Cloud Use Cases Version 1.0. 08 May 2012. OASIS Committee Note 01. http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/cn01/IDCloud-usecases-v1.0-cn01.html.

Table of Contents

Table of Figures

1 Introduction

1.1 Statement of Purpose

Cloud Computing is turning into an important IT service delivery paradigm. Many enterprises are experimenting with cloud computing, using clouds in their own data centers or hosted by third parties, and increasingly they deploy business applications on such private and public clouds. Cloud Computing raises many challenges that have serious security implications. Identity Management in the cloud is such a challenge.

Many enterprises avail themselves of a combination of private and public Cloud Computing infrastructures to handle their workloads. In a phenomenon known as "Cloud Bursting", the peak loads are offloaded to public Cloud Computing infrastructures that offer billing based on usage. This is a use case of a Hybrid Cloud infrastructure. Additionally, governments around the world are evaluating the use of Cloud Computing for government applications. For instance, the US Government has started apps.gov to foster the adoption of Cloud Computing. Other governments have started or announced similar efforts.

The purpose of the OASIS Identity in the Cloud TC is to collect and harmonize definitions, terminologies, and vocabulary of Cloud Computing, and develop profiles of open standards for identity deployment, provisioning and management. Where possible, the TC will seek to re-use existing work. The TC will collect use cases to help identify gaps in existing Identity Management standards. The use cases will be used to identify gaps in current standards and investigate the need for profiles for achieving interoperability within current standards, with a preference for widely interoperable and modular methods.

Additionally, the use cases may be used to perform risk and threat analyses. Suggestions to mitigate the identified risks and the threats and vulnerabilities will be provided.

The TC will focus on collaborating with other OASIS Technical Committees and relevant standards organizations such as The Open Group, Cloud Security Alliance and ITU-T in the area of cloud security and Identity Management. Liaisons will be identified with other standards bodies, and strong content-sharing arrangements sought where possible, subject to applicable OASIS policies.

1.2 References

The following references are used to provide definitions of and information on terms used throughout this document:

[Needham78]

R. Needham et al. *Using Encryption for Authentication in Large Networks of Computers*. Communications of the ACM, Vol. 21 (12), pp. 993-999. December 1978.

[NIST-SP800-145]

P. Mell, T. Grance, *The NIST Definition of Cloud Computing SP800-145*. National Institute of Standards and Technology (NIST) - Computer Security Division – Computer Security Resource Center (CSRC), January 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[REST-Def]

Fielding, Architectural Styles and the Design of Network-based Software Architectures. 2000. http://www.ics.uci.edu/~fielding/pubs/dissertation/top.

[RFC 1510]

IETF RFC, J. Kohl, C. Neuman. *The Kerberos Network Authentication Requestor (V5)*. IETF RFC 1510, September 1993. http://www.ietf.org/rfc/rfc1510.txt.

[RFC 1738]

IETF RFC, Berners-Lee, et. al., *Uniform Resource Locators (URL)*, IETF RFC 1738, December 1994. http://www.ietf.org/rfc/rfc1738.txt

[RFC 3986]

IETF RFC, Berners-Lee, et. al., Uniform Resource Locators (URL), IETF RFC 3986, January 2005. *http://tools.ietf.org/html/rfc3986*

[RFC 4949]

R. Shirley. et al., *Internet Security Glossary, Version 2*, IETF RFC 4949, August 2009. http://www.ietf.org/rfc/rfc4949.txt.

[SAML-Core-2.0]

OASIS Standard, *Security Assertion Markup Language 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.

[SAML-Gloss-2.0]

OASIS Standard, *Glossary for the OASIS Security Assertion Markup Language (SAML)* V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf.

[W3C-XML]

W3C Extensible Markup Language (XML) Standard homepage. http://www.w3.org/XML/

[W3C-XML-1.0]

W3C Recommendation, *Extensible Markup Language (XML) 1.0 (Fifth Edition),*26 November 2008. http://www.w3.org/TR/xml/

[X.idmdef]

Recommendation ITU-T X.1252, *Baseline identity management terms and definitions*, International Telecommunication Union – Technical Communication Standardization Sector (ITU-T), April 2010. http://www.itu.int/rec/T-REC-X.1252-201004-I/

2 Use Case Composition

Use cases have been submitted from various TC members, but for ease of consumption and comparison, each has been presented using an agreed upon "Use Case Template" (described below) along with notable categorizations.

2.1 Use Case Template

Each use case is presented using the following template sections:

- Description / User Story
- Goal or Desired Outcome
- Categories Covered
  - Categories Covered
  - Applicable Deployment and Service Models
  - Actors
  - Systems
  - Notable Services
  - Dependencies
  - Assumptions
- Process Flow

2.1.1 Description / User Story

This section contains a general description of the use case in consumer language that highlights the compelling need for one or more aspects of Identity Management while interacting with a cloud deployment model.

2.1.2 Goal or Desired Outcome

A general description of the intended outcome of the use case including any artifacts created.

2.1.3 Notable Categorizations and Aspects

A listing of the Identity Management categories covered by the use case (as identified in section XXX)

2.1.4 Featured Deployment and Service Models

This category contains a listing of one or more the cloud deployment or service models that are featured in the use case. The use case may feature one or more deployment or service models to present a concrete use case, but still be applicable to additional models. The deployment and service model definitions are those from **[NIST-SP800-145]** unless otherwise noted.

These categories and values include:

- **Featured (Cloud) Deployment Models**

  - **Private**
  - **Public**
  - **Community**
  - **Hybrid**
  - ***None featured*** – This value means that use case may apply to any cloud deployment model.
- **Featured Service Models**
  - **Software-as-a-Service (SaaS)**
  - **Platform-as-a-Service (PaaS)**
  - **Infrastructure-as-a-Service (IaaS)**
  - ***Other*** (i.e. other "as-a-Service" Models) – This value indicates that the use case should define it's specific service model within the use case itself.
  - ***None featured*** – This value means that the use case may apply to any cloud deployment model.

2.1.5 Actors

This category lists the actors that take part in the use case. These actors describe humans that perform a role within the cloud use case and should be reflected in the Process Flow section of each use case.

2.1.6 Notable Services

A category lists any services (security or otherwise) that significantly contribute to the key aspects of the use case.

2.1.7 Systems

This category lists any significant entities that are described as part of the use case, but do not require a more detailed description of their composition or structure in order to present the key aspects of the use case.

2.1.8 Dependencies

A listing of any dependencies the use case has as a precondition.

2.1.9 Assumptions

A listing of any assumptions made about the use case including its actors, services, environment, etc.

2.1.10 Process Flow

This section contains a detailed, stepwise flow of the significant actions that comprise the use case.

2.2 Identity Management Categorizations

This section defines identity management categorizations that are featured in the use cases presented in this document. Use cases may list one or more of these categorizations within the “Categories Covered” box of the “Notable Categorizations and Aspects” section of each use case.

This document will use the following categories to classify identity in the cloud use cases:

- Infrastructure Identity Establishment
- Identity Management (IM)
  - General Identity Management
  - Infrastructure Identity Management (IIM)
  - Federated Identity Management (FIM)
- Authentication
  - General Authentication
  - Single Sign-On (SSO)
  - Multi-factor
- Authorization
- Account and Attribute Management
  - Account and Attribute Provisioning
- Security Tokens
- Governance
- Audit and Compliance

2.2.1 Infrastructure Identity Establishment

This category includes use cases that feature establishment of identity and trust between cloud providers their partners and customers and includes consideration of topics such as Certificate Services (e.g. x.509), Signature Validation, Transaction Validation, Non-repudiation, etc..

2.2.2 Identity Management (IM)

This category includes use cases that feature Identity Management in cloud deployments.

2.2.2.1 General Identity Management

This categorization is used if the use case features the need for Identity Management in general terms without specify or referencing particular methods or patterns.

2.2.2.2 Infrastructure Identity Management (IIM)

This subcategory includes use cases that feature Virtualization, Separation of Identities across different IT infrastructural layers (e.g. Server Platform, Operating System (OS), Middleware, Virtual Machine (VM), Application, etc).

2.2.2.3 Federated Identity Management (FIM)

This subcategory includes use cases that feature the need to federate Identity Management across cloud deployments and enterprise.

2.2.3 Authentication

This category includes use cases that describe user and service authentication methods applicable to cloud deployments.

2.2.3.1 General Authentication

This categorization is used if the use case features the need for Authentication in general terms without specify or referencing particular methods or patterns.

2.2.3.2 Single Sign-On (SSO)

This subcategory of authentication includes use cases that feature Single Sign-On (SSO) patterns across cloud deployment models.

2.2.3.3 Multi-Factor Authentication

This subcategory of authentication indicates the use cases uses more than one factor or credential to establish the identity of a user or service. The more factors that can be verified or authenticated about an identity the greater the weight or "strength" is given to the authenticated identity; this causes an association to the term "strong authentication".

2.2.4 Authorization

This category features use cases that feature granting of Access Rights to cloud resources to users or services following establishment of identity. Use cases in this section may include authorization concepts such as Security Policy Enforcement, Role-Based Access Control (RBAC) and representations and conveyance of authorization such as Assertions to cloud services.

2.2.5 Account and Attribute Management

This category includes use cases that feature account establishment including Security Policy Attributes along with their Management or Administration. Use cases may include descriptions of established provisioning techniques, as well as developing examples of Just-In-Time (JIT) Account Provisioning.

2.2.5.1 Account and Attribute Provisioning

This subcategory of Account and Attribute Management highlights use cases that feature provisioning of identity and accounts within cloud deployments. This includes provisioning of any attributes that are associated with an identity that may affect policy decisions and enforcement.

2.2.6 Security Tokens

This category includes use cases that feature Security Token Formats and Token Services including Token Transformation and Token Proofing.

2.2.7 Governance

This category includes the secure management of identities and identity related information (including privacy information) so that actions taken based on those identities can be legally used to validate adherence to the rules that define the security policies of the system.

2.2.8 Audit & Compliance

This category includes use cases that feature Identity Continuity within cloud infrastructure and across cloud deployment models for the purpose of non-repudiation of identity associated with an action permitted against security policy.

2.3 Actor Name Construction

In order to have consistent names for actors (roles) referenced in use cases, this document defines qualification syntax comprising four terms.

This syntax is intended to provide a detailed context of where the actor is performing their use case function, under which organization, against what resources and under what role.

These four terms are:

- **Deployment Type** – Qualifies the actor's domain of operation (i.e. the deployment entity where they perform their role or function).
- **Organizational Type** – Further qualifies the actor by the organization within their deployment entity
- **Resource Type** – Further Qualifies the actor by the resources they have been entitled to interact with.
- **Role Type** – Further qualifies the actor by their role-based entitlements.

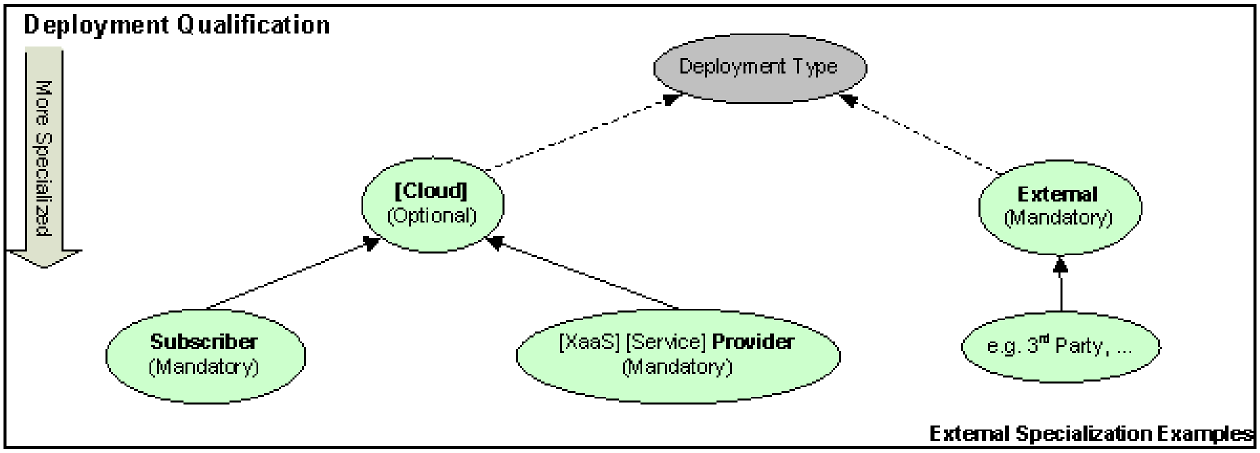
The general syntax for creating a name for an actor is as follows:

Deployment Type | Organizational Type | Resource Type | Role Qualification

The following sections include diagrams that show the logical derivation (inheritance) for each of these qualification terms.

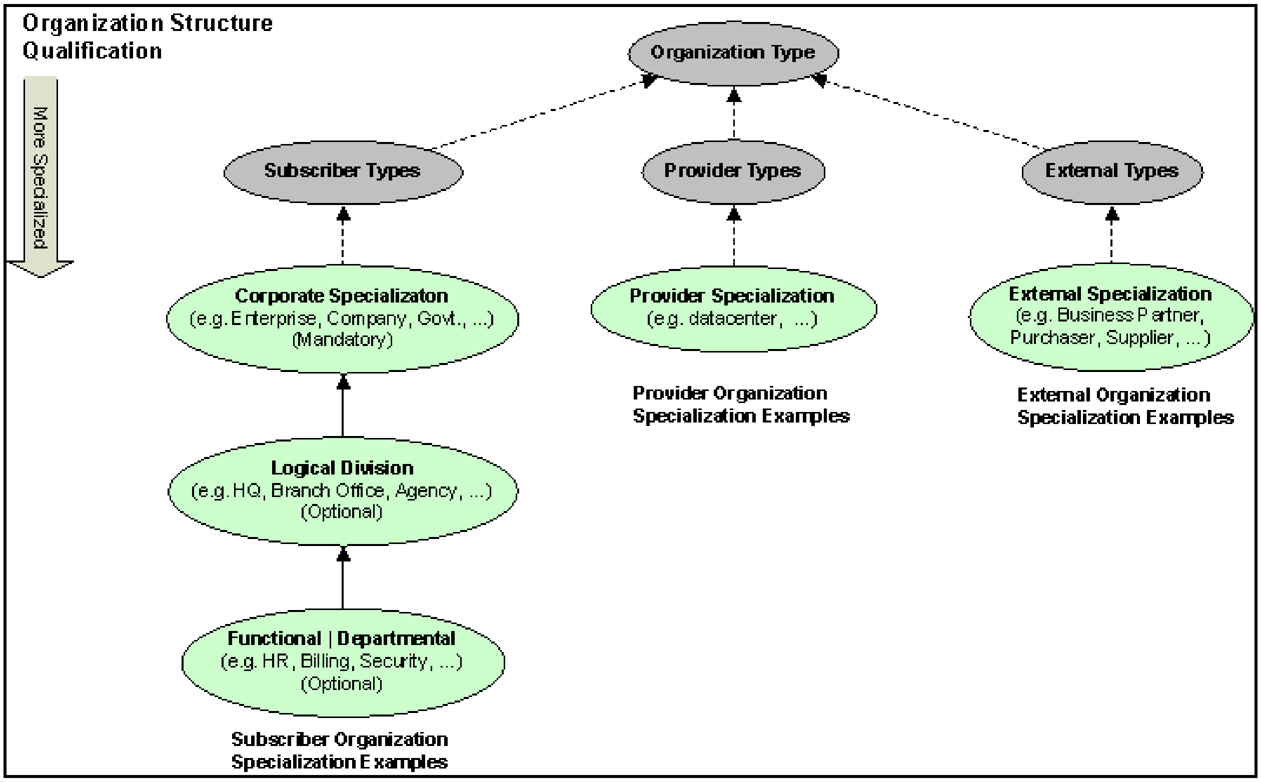
2.3.1 Deployment Qualifications

The following diagram shows the deployment types that are required when naming an actor:



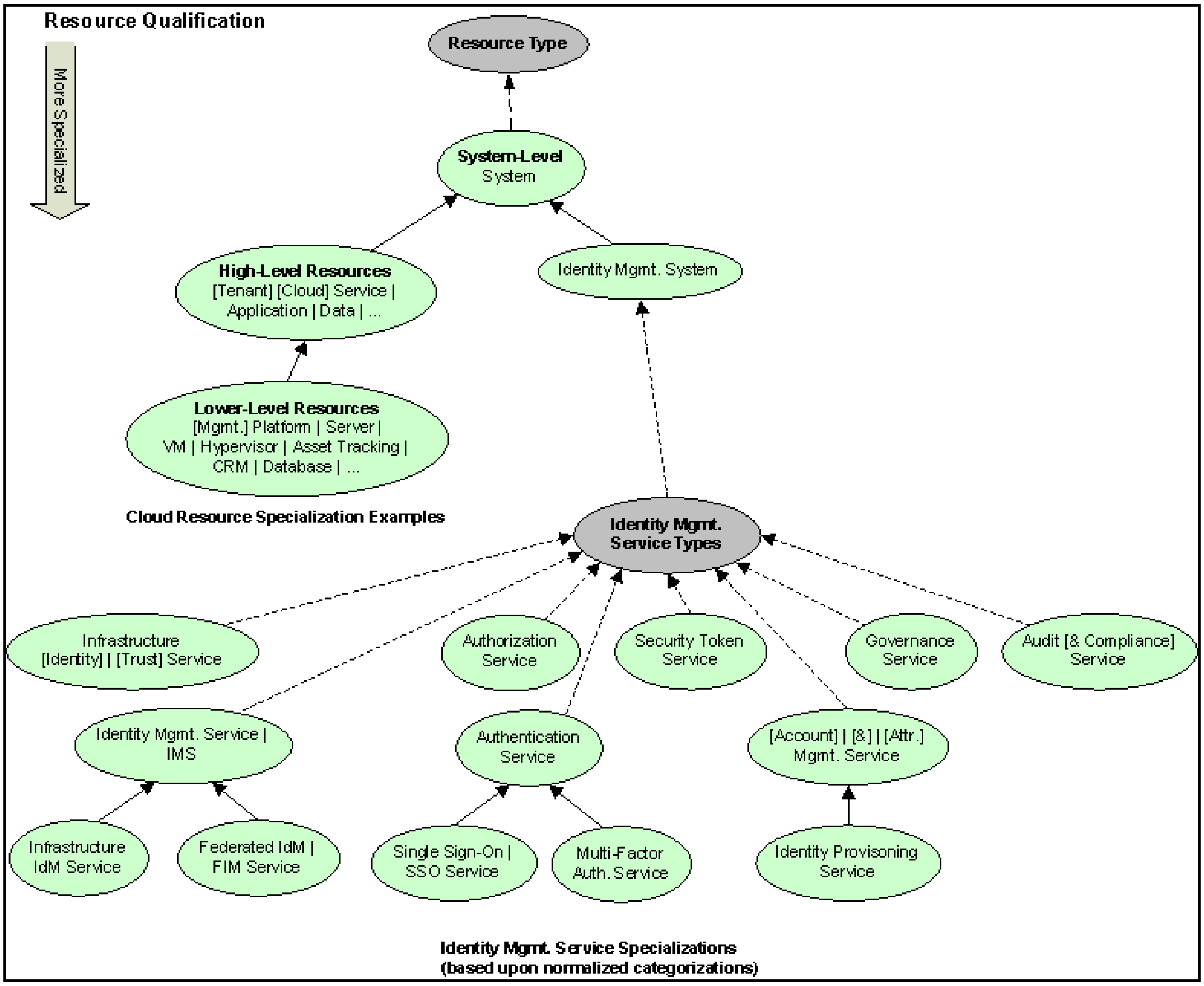
2.3.2 Organization Qualifications

The following diagram shows the organizational types that are required when naming an actor:


Organization Structure Qualification
More Specialized
Organization Type
Subscriber Types
Provider Types
External Types
Corporate Specializaton (e.g. Enterprise, Company, Govt., ...) (Mandatory)
Provider Specialization (e.g. datacenter, ...)
External Specialization (e.g. Business Partner, Purchaser, Supplier, ...)
Provider Organization Specialization Examples
External Organization Specialization Examples
Logical Division (e.g. HQ, Branch Office, Agency, ...) (Optional)
Functional | Departmental (e.g. HR, Billing, Security, ...) (Optional)
Subscriber Organization Specialization Examples

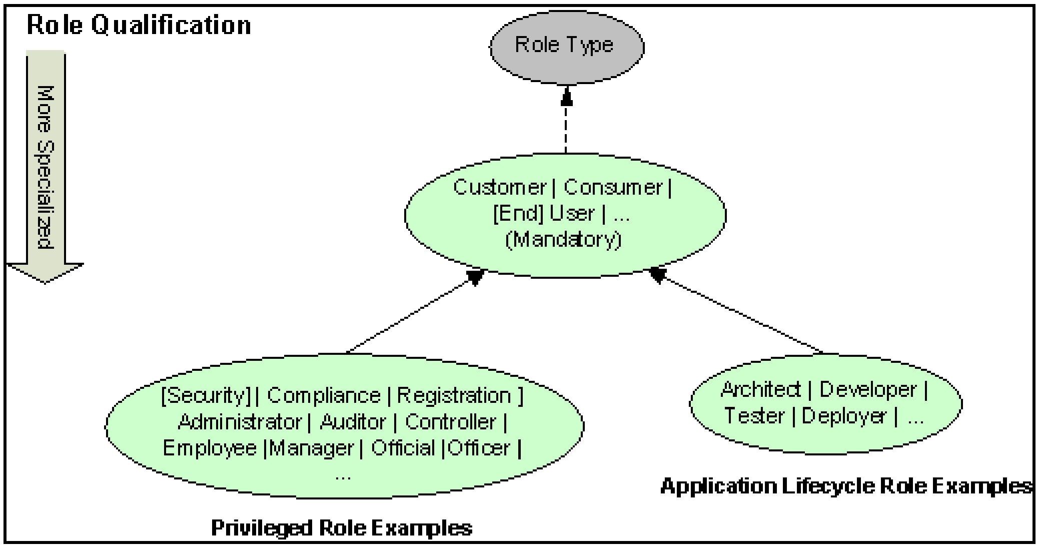
2.3.3 Resource Qualifications

The following diagram shows the resource types that are required when naming an actor:



2.3.4 Role Qualifications

The following diagram shows the role types that are required when naming an actor:


Role Qualification
More Specialized
Role Type
Customer | Consumer | [End] User | ... (Mandatory)
[Security] | Compliance | Registration] Administrator | Auditor | Controller | Employee |Manager | Official |Officer | ...
Architect | Developer | Tester | Deployer | ...
Application Lifecycle Role Examples
Privileged Role Examples

2.4 Service Name Construction

In order to have consistent names for services referenced in use cases, this document defines qualification syntax comprised of three terms.

This syntax is intended to provide a detailed context of which deployment a service is running in and which resources it is providing (access to).

The three terms are:

- **Deployment Type** – Qualifies the actor's domain of operation (i.e. the deployment entity where they perform their role or function).
- **Organizational Type** – Further qualifies the actor by the organization within their deployment entity
- **Resource Type** – Further Qualifies the actor by the resources they have been entitled to interact with.

The general syntax for creating a name for a service is as follows:

Deployment Type | Organizational Type | Resource Type

The section presented above titled "Actor Name Construction" includes diagrams that show the logical derivation (inheritance) for each of these qualification terms. The naming or qualification of services is approached in the same way as in naming an actor; however, a service does not require a "role" qualification.

Note: The syntax described here for naming services also provides guidance for naming system resources and sets of services that define systems within use cases.

3 Use Case Overview

This section contains an overview of the use cases provided by the use cases presented in the next section along with identity and deployment classification information.

3.1 Use Case Listing and Description of Goals

The following table provides an overview of the use cases presented in this document.

Use Case #	Title	Goals Description Comments
1	Application and Virtualization Security	Feature the importance of managing identities that exist in cloud at all levels, including the host operating system, virtual machines as well as applications. Ownership and management of identities may vary at each level and also be external to the cloud provider.
2	Identity Provisioning	Feature the need support and manage customer policies for identity decommissioning including transitioning of affected resources to new identities.
3	Identity Audit	Feature the importance of auditing/logging of sensitive operations performed by users and administrators in the cloud.
4	Identity Configuration	Feature the need for portable standards to configure identities in cloud applications and infrastructure (virtual machines, servers etc).
5	Middleware Container in a Public Cloud	Show how cloud identities need to be administered and accounted for in order to manage middleware containers and their applications.
6	Federated SSO and Attribute Sharing	Feature the need for Federated Single Sign-On (F-SSO) across multiple cloud environments.
7	Identity Silos in the Cloud	Exhibit how identity attributes can be aggregated based on multiple silos within a cloud, a group of clouds or from outside the cloud.
8	Identity Privacy in a Shared Cloud Environment	Show the need for controls to exist to maintain privacy of identities while operating in a cloud if desired.
9	Cloud Signature Services	There is a business need in many applications to create digital signatures on documents and transactions. When

Use Case #	Title	Goals Description Comments
		applications, and users, move into the cloud so should also the signing services. Both users and applications have a need to sign documents.
10	Cloud Tenant Administration	Feature the ability for enterprises to securely manage their use of the cloud provider's services (whether IaaS, PaaS or SaaS), and further meet their compliance requirements. Administrator users are authenticated at the appropriate assurance level (preferably using multi-factor credentials).
11	Enterprise to Cloud SSO	A user is able to access resource within their enterprise environment or within a cloud deployment using a single identity. With enterprises expanding their application deployments using private and public clouds, the identity management and authentication of users to the services need to be decoupled from the cloud service in a similar fashion to the decoupling of identity from application in the enterprise. Users expect and need to have their enterprise identity extend to the cloud and used to obtain different services from different providers rather than multitude of userid and passwords. By accessing services via a federated enterprise identity, not only the user experience of SSO is to gain, but also Enterprise compliance and for control of user access, ensuring only valid identities may access cloud services.
12	Consumer Cloud Identity Management, Single Sign-On (SSO) and Authentication	A user (or cloud consumer) is able to access multiple SaaS applications using a single identity.
13	Transaction Validation and Signing in the Cloud	Users are able to perform transaction and document signing in the cloud using a trusted signing service that manages their signing keys.
14	Enterprise Purchasing from a Public Cloud	Reduce the number of passwords that are stored and used in the cloud and eliminate the need for cloud "directory synchronization" while advocating a "claims based"

Use Case #	Title	Goals Description Comments
		architecture.
15	Access to Enterprise's Workforce Applications Hosted in Cloud	Exhibit the need for seamless authentication and access privileges conveyance from an enterprise that is wishes to host their workforce applications on a public cloud.
16	Offload Identity Management to External Business Entity	Show the need for federated identity management which enables an enterprise to make available cloud-hosted applications to either the employees of its customers & business partners or its own institutional consumers and avoid directly managing identities (accounts) for those users.
17	Per Tenant Identity Provider Configuration	Show the need for cloud tenants to securely manage cloud services using automated tools rather than navigating and manually configuring each service individually.
18	Delegated Identity Provider Configuration	Show the need for cloud tenant administrators need to delegate access to their identity services configuration within a multi-tenant cloud service to their chosen identity provider service.
19	Auditing Access to Company Confidential Videos in Public Cloud	Features the need to audit various role-based accesses of a confidential data objects stored in a public cloud against the owning company's security policy
20	Government Provisioning of Cloud Services	Show how authorized government personnel could be granted access and assigned appropriate privileges to configure and provision a cloud service.
21	Mobile Customers' Identity Authentication Using a Cloud provider	Show how a financial company is able to use a cloud service provider to authenticate its globally-based mobile clients and to connect them to the closest (cloud) physical location for fast response.
22	Cloud-based Two-Factor Authentication Service	Exhibits the value of a Two-Factor Authentication (2FA) cloud-based service that can be used with an Identity Provider, deployed either at the enterprise, at the cloud service provider, or as a separate cloud service
23	Cloud Application Identification using Extended Validation Certificates	Shows the value of providing validatable identification of the Cloud Provider/SaaS application to the user or consumer using Extended Validation (EV) certificates.

Use Case #	Title	Goals Description Comments
24	Cloud Platform Audit and Asset Management using Hardware-based Identities	Describes the value of ``proof of execution'' using persistent hardware-based identities that are traceable and logged as part of the audit trail for the Enterprise customer.
25	Inter-cloud Document Exchange and Collaboration	Businesses trading with one another should be able to seamlessly establish new electronic trading relationships via their existing cloud application and commerce systems. In particular, the identities, attributes and relationships required on the various systems should be able to be set up with zero or minimal user intervention.
26	Identity Impersonation / Delegation	Customers of the cloud provider may require a cloud provider to supply support that permits one identity to impersonates the identity of another customer without sacrificing security
27	Federated User Account Provisioning and Management for a Community of Interest (CoI)	Show the need for provisioning, administration and governance of user identities and their attributes for organizations that have a distributed structure which includes many central, branch offices and business partners where each may utilize cloud deployment models.
28	Cloud Governance and Entitlement Management	Provide a means for external identity governance by cloud consumers so that they can inspect and manage assignable entitlements for cloud provider SaaS or PaaS applications, as well as for cloud hosted consumer accounts. That there is a need to do this in a standard way so that entitlements can be modeled and understood for audit and provisioning purposes.
29	User Delegation of Access to Personal Data in a Public Cloud	Users are able to dynamically delegate (grant and revoke) and constrain access to files or data stored with a cloud service provider to users whose identities are managed by external identity providers.

3.2 Use Case Coverage by Identity Management Categorizations

The following table shows which Identity Management Categorizations are featured in which use cases as described in section Identity Management Categorizations.

Key: A letter “P” in a column indicates that the category is a primary aspect featured in the use case where an “S” indicates a Secondary categorization for the use case.

Use Case #	Infra. Identity Est.	Identity Mgmt.			Authentication			Authorization	Account / Attribute Mgmt.		Security Tokens	Governance	Audit & Compliance
		Gen.	*IIM*	*FIM*	*Gen.*	*SSO*	*Multi-Factor*		*Gen.*	*Provisioning*			
1		P	P	S					S				
2		P							P				
3													P
4		P							S				
5		P			P			P					
6					P	P		S		S	S		
7				P	S			S	S				
8									P			P	
9					P			S					
10							P	P					S
11				P	P	P							
12				P	P	P							
13		P			P								S
14	P					P		S			S		
15				P	S			S					
16				P	S			S	S				
17	P			P									
18	P				S			S	S				
19						S		S					P
20					P			S					S
21				S	P	S							
22	P					P			S				
23	P												
24	P												P
25				P	P			S	S	S			
26		P			P				S				S
27		S		P					P	P			
28									S	S		P	P
29				S	P			P		S		P	

3.3 Use Cases Featuring Cloud Deployment or Service Models

Key: Use cases that intend to feature particular Cloud Deployment or Service Models will have a mark under the respective model names to denote that intention.

Note: Use cases that are not featuring a particular Cloud Deployment Model will have a mark in the "None" column. This can be interpreting as meaning the use case is valid for all defined Cloud Deployment Models.

Note: Use cases that are not featuring a particular Cloud Service Model will have a mark in the "None" column. This can be interpreting as meaning the use case is valid for all defined Cloud Service Models.

Use Case #	**Featured Cloud Deployment Models**					**Featured Cloud Service Models**				
	None	***Private***	***Public***	***Community***	***Hybrid***	***None***	***SaaS***	***PaaS***	***IaaS***	***Other***
1		X	X					X	X	
2	X						X			
3	X					X				
4	X					X				
5			X						X	
6	X					X				
7	X					X				
8	X					X				
9	X					X				
10			X				X	X	X	
11	X					X				
12			X	X			X			
13			X			X				
14			X				X			
15	X						X			
16	X						X			
17	X					X				
18	X					X				
19			X						X	
20	X					X				
21		X	X				X	X	X	
22	X					X				
23	X						X			
24		X	X						X	
25					X				X	
26	X					X				
27				X	X		X			
28			X				X	X		

29			X						X	

4 Use Cases

4.1 Use Case 1: Application and Virtualization Security in the Cloud

4.1.1 Description / User Story

Cloud Computing environments have one or more virtual machines/images running on a Host Operating system on a server. Applications run inside these virtual machines (guest operating systems). Applications can run directly on the host operating system. Identities can be associated with each of these virtual machines. Identities can be associated with the applications running on that server (including the virtual machines).

Virtual Machines can be owned by different owners. We have identities that administer the virtual machines. We have identities that use the applications. The Virtual Machine identities may not be the same as the application identities (and that each identity may have managed by different Identity Management services). Authentication and validation of Identities by the cloud infrastructure may not be sufficient for the owners of virtual machines.

4.1.2 Goal or Desired Outcome

Since a cloud server can have multiple virtual machines and applications run on these guest operating systems, it is important to manage the identities that exist in the host operating system, virtual machines as well as applications. Additionally, it should be possible for VM owners to do their own proofing of identities.

There is an understanding that there is a need for separation of identities within a cloud infrastructure and that these identities are not all owned by the cloud provider (e.g. more than one identity service).

4.1.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ Infrastructure Identity Mgmt. ○ General Identity Mgmt. • Secondary: ○ Federated Identity Mgmt. (FIM) ○ Account and Attribute Mgmt.	**Featured Deployment and Service Models:** • Deployment Models ○ Private ○ Public • Service Models ○ Platform-as-a-Service (PaaS) ○ Infrastructure-as-a-Service (IaaS)
Actors: • Subscriber Company Server Administrator. • Subscriber Company Virtual Machine	**Systems:** • Cloud Provider Identity Mgmt. System, helps manage resources such as:

Owner • Subscriber Company Virtual Machine Administrator • Subscriber Company Application Deployer • Subscriber Company Application User	• Cloud Identity Stores
Notable Services: • Federated Identity Mgmt. Service	
Dependencies: • None	
Assumptions: • The Cloud Provider's Identity Mgmt. System is able to provide management of identities for various cloud-based resources (e.g. Virtual Servers, their Host Operating Systems, Virtual Machines, etc.) including authentication, validation and persistence (e.g. to a Cloud Identity Store). • The Cloud Provider's Identity Mgmt. System is able to transform a Federated Identity to a cloud-local identity by providing a Federated Identity Mgmt. Service. • Multi-Tenancy ○ Multiple Virtual Machines may be deployed and run on a single host operating system. ○ Not all virtual machines running on a single host operating system is owned by a single entity.	

4.1.4 Process Flow

1. A Subscriber Company's Server Administrator (One type of cloud identity) administers a virtual server in the cloud. He has privileges to administer the cloud-based host operating system and its services.
2. A Subscriber Company's Virtual Machine (VM) Owner Virtual Machine Administrator (another cloud identity) commissions a Virtual Machine to run on the virtual server.
3. A Subscriber Company's Application Deployer (another type of cloud identity) then deploys an application on the Virtual Machine running in the cloud.
4. A Subscriber Company's Application User (another type cloud identity) then makes use of this cloud-hosted application.
5. The Subscriber Company's Server Administrator, Virtual Machine Owner, Application Owner and Application User identities are authenticated/validated/transformed against an Identity Management System that is provided by the cloud (i.e. a Cloud Provider Identity Mgmt. System).
6. The Cloud Provider's Identity Mgmt. System can transform a Federated Identity to a local identity, if needed, by providing Federated Identity Mgmt. Services.

4.2 Use Case 2: Identity Provisioning

4.2.1 Description / User Story

Resources exist in the cloud. These resources can be virtual machines running on a server, applications running inside a virtual machine or a document created/stored on a public cloud.

Eventually, the cloud identities that own these resources may get decommissioned. If the link between the resource and its decommissioned owner is lost, it is possible that the particular resource is lost for ever. Ideally, facilities via design should exist to transition the resources to new owners.

As an example consider the case when an employee creates company documents in a public cloud. These are official company documents hosted on a public cloud infrastructure. Now when the employee leaves the company, his employer should be able to transition the documents to another employee.

4.2.2 Goal or Desired Outcome

When identities get decommissioned, the resources owned by these identities (including virtual machine images and related data) should not be automatically decommissioned. There should be facilities and policies available to transition these resources to new identities.

4.2.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ General Identity Mgmt. ○ Account and Attribute Mgmt. • Secondary ○ None	**Featured Deployment and Service Models:** • Deployment Models ○ None featured • Service Models ○ Software-as-a-Service (SaaS)
Actors: • Subscriber Company Application Administrator • Subscriber Company Application User	**Systems:** • Cloud Provider Identity Mgmt. System, helps manage resources such as: ○ Cloud Identity Stores
Notable Services: • Cloud Applications • Cloud Identity Stores	
Dependencies: • None	
Assumptions: • None	

4.2.4 Process Flow

1. A Subscriber Company's Application User, an employee of the company, creates multiple resources within a cloud deployment.
2. The Subscriber Company's Application User that created these cloud resources leaves the company.

3. The Subscriber Company’s Application Administrator decommissions the Application User’s identity within the cloud deployment.
4. The Subscriber Company’s Application Administrator transitions the cloud resources to a different employee’s identity within the same cloud deployment.

4.3 Use Case 3: Identity Audit

4.3.1 Description / User Story

Users and administrators of the cloud environment perform security sensitive operations. There is a need to audit their actions in a tamper proof fashion.

4.3.2 Goal or Desired Outcome

For compliance purposes, it is important to audit/log sensitive operations performed by users and administrators in the cloud environment.

4.3.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ Audit and Compliance • Secondary ○ None	**Featured Deployment and Service Models:** • Deployment Models ○ None featured • Service Models ○ None featured
Actors: • Subscriber Company Application Administrator • Subscriber Company Application User	**Systems:** • Cloud Provider Identity Mgmt. System, helps manage resources such as: ○ Cloud Identity Stores
Notable Services: • Cloud Auditing Service	
Dependencies: • Common Logging/Auditing standards.	
Assumptions: • The Provider’s Cloud Auditing Service is able to log/audit sensitive operations on Cloud Applications and work with Provider’s Identity Mgmt. System (e.g. Cloud Identity Store) log the identifies used to perform them.	

4.3.4 Process Flow

1. The Subscriber Company’s Application Administrator manages a Cloud Application within a cloud deployment.

2. A Subscriber Company's Application User, an employee of the company, interacts with the Cloud Application.
3. The Cloud Provider provides a Cloud Auditing Service that supports a common auditing standard that is used to log all sensitive operations happening in the cloud environment.
4. The log contains the operations and identities of both the Subscriber Company's Application Administrator and User against the Cloud Application.

4.4 Use Case 4: Migration of Identity & Attributes between Cloud Providers

4.4.1 Description / User Story

Cloud Applications use identities. The cloud infrastructure uses identities. If there is a configuration that is an accepted standard, then it is easier to migrate the configuration across cloud infrastructures. This type of migration is desirable to permit subscribers the ability easily move applications between cloud deployment types and between cloud providers without loss of the identities associated with the applications.

4.4.2 Goal or Desired Outcome

Portable standards exist for configuration of identities in the applications and the infrastructure (virtual machines, servers etc).

4.4.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ General Identity Mgmt. • Secondary ○ Account and Attribute Mgmt.	**Featured Deployment and Service Models:** • Deployment Models ○ None featured • Service Models ○ None featured
Actors: • Subscriber Company Application Administrator	**Systems:** • Cloud Provider Identity Mgmt. System, helps manage resources such as: ○ Cloud Applications ○ Cloud Identity Stores ○ Cloud Metadata Services
Notable Services: ○ Cloud Provisioning Service	
Dependencies: • Standards based configuration template (for provisioning identities)	
Assumptions:	

- Cloud Provider's Identity Mgmt. System provides services (e.g. a Cloud Provisioning Service) that enable Subscriber Cloud Application Administrators to load (provision) identities that are permitted to interact with a Cloud Application.

4.4.4 Process Flow

1. A company's application administrator is able to use a standard configuration template to load identities into a cloud application from the Cloud Provider's Identity Management System.
2. Similarly a standard configuration template is used to load (provision) the subscriber's identities for the cloud application.

4.5 Use Case 5: Middleware Container in a Public Cloud Infrastructure

4.5.1 Description / User Story

Middleware containers are services that are able to host applications on a server. A middleware container such as a Java EE Application Server can run on a virtual machine in the cloud. Administrator identities can exist to manage these middleware containers. Deployer identities may exist to manage the deployment lifecycle of applications running in the middleware containers. In a clustered environment, a middleware set up may spawn multiple virtual machines across one or more servers.

4.5.2 Goal or Desired Outcome

Identities are accounted and administered by the cloud to manage middleware containers and their applications.

4.5.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ General Identity Management (IM) ○ General Authentication ○ Authorization • Secondary ○ None	**Featured and Service Models:** • Deployment Models ○ Public • Service Models ○ Infrastructure-as-a-Service (IaaS)
Actors: • Subscriber Middleware Administrator • Subscriber Middleware Deployer • Subscriber Application User	**Systems:** • Cloud Provider Identity Mgmt. System, helps manage resources such as: ○ Cloud Applications ○ Cloud Identity Stores
Notable Services: • Cloud Provider Authentication Service	

• Cloud Provider Authorization Service
Dependencies: • None
Assumptions: • None

4.5.4 Process Flow

1. A Subscriber's Middleware Administrator creates a middleware container on a virtual machine.
2. A Subscriber's Middleware Deployer then manages the deployment of applications on this middleware container.
3. The Provider's Cloud Authentication and Authorization services are used to authenticate and authorize the identities.

4.6 Use Case 6: Federated Single Sign-On and Attribute Sharing

4.6.1 Description / User Story

There are multiple applications hosted in the cloud. If you view a cloud as a single security domain, then a collection of cloud environments encompass multiple security domains. A user in one domain should be able to access applications hosted in another cloud or domain as long as a trust relationship exists between the two cloud environments.

Additionally, for users coming in from external cloud or domains, it should be possible to map (or transform) identity attributes to the local environment.

4.6.2 Goal or Desired Outcome

Federated Single Sign-On (SSO) is achieved with multiple cloud environments.

4.6.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ General Authentication ○ Single Sign-On (SSO) • Secondary ○ Authorization ○ Account and Attribute Provisioning ○ Security Tokens	**Applicable Deployment and Service Models:** • Featured Deployment Models ○ None featured • Featured Service Models ○ None featured
Actors:	**Systems:**

• Subscriber Cloud Application Administrator • External Cloud Application User	• Cloud Provider Identity Mgmt. System, helps manage resources such as: ○ Cloud Applications ○ Cloud Identity Stores
Notable Services: • Cloud Provider Identity Mgmt. Service • Cloud Provider Attribute Service (for transformation) • Cloud Provider Authorization Service	
Dependencies: • None	
Assumptions: • Federated identities (standards) supporting Single Sign-On (SSO) • The same federated identity can be used with different cloud providers (i.e. identity can be localized).	

4.6.4 Process Flow

1. An (external) end user of a cloud based application attempts to access an application in the cloud. The call comes with a federated identity attached.
2. The Cloud Provider Identity Mgmt. Service accepts the federated identity of the end user and performs the necessary transformation to cloud provider defined attributes (using the Cloud Provider's Attribute Service).

   2.1. There may be several back channel operations between the end user's and the cloud providers Identity Mgmt. System to accomplish the necessary attribute transformation.
3. Locally defined access to the application in the cloud is provided.
4. The external end user is able to use their new local identity to access the cloud application.

4.7 Use Case 7: Identity Silos in the Cloud

4.7.1 Description / User Story

Identity information can be persisted in stores such as a directory (e.g. LDAP) within a single cloud computing environment, multiple cloud environments or outside the cloud (perhaps at the enterprise).

4.7.2 Goal or Desired Outcome

Identity attributes can be aggregated based on multiple silos within a cloud, a group of clouds or from outside the cloud.

4.7.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ Federated Identity Mgmt. (FIM) • Secondary ○ General Authentication ○ Authorization ○ Account and Attribute Mgmt.	**Featured Deployment and Service Models:** • Deployment Models ○ None featured • Service Models ○ None featured
Actors: • Subscriber Company Employee	**Systems:** • Cloud Provider Identity Management System, helps manage resources such as: ○ Cloud Applications ○ Cloud Identity Stores (or Directory Service)
Notable Services: • Cloud Provider Attribute Services	
Dependencies: • None	
Assumptions: • Standards for Federated Identity Management that permit identity attributes to be aggregated and transformed for use within the cloud.	

4.7.4 Process Flow

1. A Subscriber Company Employee accesses an application in the cloud.
2. The Cloud Provider Identity Management System infrastructure has to authenticate, authorize and proof this user based on information stored in its directory servers as well as get additional attributes from the employer's directory server or any attribute service that exists outside the cloud.

   2.1. The Provider Identity Management System works with the Cloud Provider Attribute Services to aggregate and transform attributes for use in the cloud domain.

4.8 Use Case 8: Identity Privacy in a Shared Cloud Environment

4.8.1 Description / User Story

Identities operate in the cloud. Many attributes associated with the identity may be confidential and need to be protected in a multi-tenant environment. There is a need for Privacy controls and Governance frameworks in the cloud to protect the privacy of the identity.

4.8.2 Goal or Desired Outcome

Controls exist to maintain privacy of identities operating in a cloud if desired.

4.8.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ Account and Attribute Mgmt. ○ Governance • Secondary ○ None	**Applicable Deployment and Service Models:** • Featured Deployment Models ○ None featured • Featured Service Models ○ None featured
Actors: • Cloud Subscriber End User	**Systems:** • Cloud Provider Identity Management System, helps manage resources such as: ○ Cloud Applications ○ Cloud Identity Stores (or Directory Service) ○ Security and Privacy Policies
Notable Services: • Cloud Provider Security Policy Service • Cloud Provider Attribute Service	
Dependencies: • None	
Assumptions: • There exist privacy control policy standards as well as Identity Governance Framework standards	

4.8.4 Process Flow

1. A Cloud Subscriber End User accesses an application in the cloud.
2. The Cloud Provider Identity Mgmt. System authenticates and proofs the user.
3. They determine that this is a Very, Very Important Person (VVIP), perhaps a government official, whose identity (attributes) should be masked from other users in the cloud.
   - 3.1. The Cloud Provider has privacy controls to enforce Security and Privacy Policies to assure that such users identities are protected (perhaps against a license agreement).
4. Appropriate privacy controls are applied such that the attributes of the identity are not visible to other users or applications in the cloud.
   - 4.1. The Cloud Providers Attribute Service is able to mask the identity attributes.

4.9 Use Case 9: Cloud Signature Services

4.9.1 Description / User Story

There is a business need in many applications to create digital signatures on documents and transactions. When applications, and users, move into the cloud so should also the signing services. Both users and applications have a need to sign documents.

- Examples as xml, pdf, odf, etc.

There are different signature standards for all these types of documents.

- Example use cases for signed documents are applications sending signed messages to other applications (e.g. Electronic Data Interchange (EDI)), corporations producing receipts or official documents (e.g. sensitive reports, tax returns. etc.) and users with need for integrity protection (e.g. agreements, purchase orders, etc).

There is also a possibility for public services, where the signature service can act as a public notary, i.e. not vouching for the contents of a message, but vouching for the integrity of the message after being signed.

4.9.2 Goal or Desired Outcome

The consumer of the signature service is authorized to sign documents, submits those and receives the signed version back. The administrator of the signature service has an auditable service, both with regards to consumer actions and administrator actions.

The signature service is typically owned by a specific entity (one identity). It is important to manage the identities of the consumers of the service, as the service may otherwise be used for message forgery. The owner and administrator identities are also vital to the security of the service.

4.9.3 Notable Categorizations and Aspects

Categories Covered: • Primary. ○ General Identity Mgmt. ○ Federated Identity Mgmt. (FIM) • Secondary: ○ Authorization ○ Account and Attribute Mgmt. ○ Audit and Compliance	**Featured Deployment and Service Models:** • Cloud Deployment Models ○ None featured • Service Models ○ Software as a Service (SaaS)
Actors: • Subscriber Cloud Application Administrator • Subscriber Company Application User • Cloud Subscriber End User	**Systems:** • Cloud Provider Identity Mgmt. System, helps manage resources such as: ○ Cloud Applications ○ Cloud Identity Stores
Notable Services: • Cloud Provider Authentication Service • Cloud Provider Authorization Service	
Dependencies:	

- Of vital importance for a signature service is authentication of users. Authentication is a prerequisite for authorization, without which signature services are virtually useless. In case of individual users there is a need to authenticate the individual and in case of organization signatures you need to identify the organizational identity of the user..

Assumptions:

- The cloud provider has the ability to securely identify Individuals and Domains (or organizations).
- Single Sign-On would be used to effectively manage authentication tokens, attributes and metadata in the cloud.
    - Signature service should be able to use the same identify as the "using" entities and services.
- Provisioning of entities should not require provisioning with the signature service itself.
- Authorization configuration would preferably not have to be done in the signature services themselves.

4.9.4 Process Flow

1. The Subscriber Company's Application Administrator manages the signature service within a cloud deployment.
2. A Cloud Subscriber End User or Subscriber Company Application User accesses the signature service in the cloud.
3. The Cloud Provider Identity Mgmt. System authenticates and proofs the user.
4. The End User is able to use their identity to access the cloud application.
5. The Cloud Authorization Service is used to authorize the End User to the specific signature service requested.
6. All operations performed by the Administrator and End User are logged for audit by the cloud provider's Cloud Application Auditing Service..

4.10 Use Case 10: Cloud Tenant Administration

4.10.1 Description / User Story

This use case demonstrates subscriber administration of an IaaS, PaaS or SaaS service in the cloud.

A subscriber business' owner (or administrator) of a company's cloud hosted service authenticates to the cloud provider's management console and is granted privileged administrative access to only its tenant application or service. Once authenticated, the user is able to perform administrative operations such as configuration of the tenant, configuration of security policies, and managing other users and their roles.

Cloud Tenant Administration is a security sensitive operation and the cloud provider must account for the privileged user access (identity) and any administrative actions they take on that particular application for security auditing purposes.

4.10.2 Goal or Desired Outcome

Goal #1: The subscriber enterprise's users can securely manage the configuration and use of the cloud hosted service while being able to rely on the provider for the audit data needed to show they meet their compliance requirements.

Goal #2: Administrator users are authenticated at the appropriate assurance level (preferably using multi-factor credentials) in order to obtain access privileges to administer the cloud service and manage their tenant application or service.

4.10.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ Multi-Factor Authentication ○ Authorization • Secondary ○ Audit and Compliance	**Featured Deployment and Service Models:** • Cloud Deployment Models ○ Public • Service Models ○ Infrastructure-as-a-Service (IaaS) ○ Platform-as-a-Service (PaaS) ○ Software-as-a-Service (SaaS)
Actors: • Subscriber Enterprise's System Administrator	**Systems:** • Cloud Identity Mgmt. System, which includes management of a: ○ Cloud Identity Store ○ Cloud Authorization/Policy Store ○ Cloud Auditing store • Subscriber's Enterprise Identify Provider (perhaps a 3rd party).
Notable Services: • Cloud Application Administration Service • Cloud Application (Multi-factor) Authentication Service • Cloud Application Authorization Service • Cloud Application Auditing Service	
Dependencies: • Prior to Authentication, the Subscriber's Cloud System or Application Administrator has set up the cloud tenant account and associated policies and provided the authentication credentials to the application business owner of band.	
Assumptions: • Privileged account already exists within the cloud that hosts the SaaS application. • Support for authentication based upon customer/consumer's organizational security policies and control requirements • The subscriber organization's (i.e. the enterprise business owner) identity is known and proofed. The use case does not cover the identity proofing process. The process is happening out of band to the use case	

- The (multi-factor) authentication process is not covered here.

4.10.4 Process Flow

1. The Subscriber Enterprise's System Administrator accesses the cloud provider's management console for the IaaS, PaaS or SaaS application.
2. The Subscriber Enterprise's System Administrator is prompted to authenticate preferably with a multi-factor authentication capability (rather than a plain userid and password). The authentication process may be provided by the cloud provider's console natively, or can be federated with the user's enterprise identity using a protocol such as SAML.
   2.1. If the cloud provider's native authentication is used for authentication, then the user is prompted for their credentials (e.g. User ID and password, or preferably multifactor credentials).
   2.2. If the subscriber's enterprise credentials are used, then the authentication process is comprised of:
      - Redirection to the Enterprise's Identity Provider (IdP)
      - Authentication using the Enterprise's approved credentials (again preferably multi-factor credentials).
      - Redirection to the SaaS application management console with the correct identity assertions.
3. Upon successful authentication, the Subscriber Enterprise's System Administrator can access the management capabilities of the cloud hosted application or service and perform privileged operations.
   3.1. The cloud provider's Cloud Application Authorization Service is used to enforce security policies (e.g. via Role Based Access Control) when accessing the SaaS application.
4. All privileged operations performed by the administrator are logged for audited by the cloud provider's Cloud Application Auditing Service.

4.11 Use Case 11: Enterprise to Cloud Single Sign-On

4.11.1 Description / User Story

This use case demonstrates how a user logs into their enterprise security services. Once authenticated the user is able to access cloud resources without the need to re-authenticate to the cloud provider.

The use case allows users to extend their enterprise identity and apply it to consuming cloud applications services in a seamless manner. With enterprises expanding their application deployments using private and public clouds, the identity management and authentication of users to the services should be decoupled from the cloud service in a similar fashion to the decoupling of identity from application in the enterprise. Users expect and need to have their enterprise identity extend to the cloud and used to obtain different services from different providers rather than logging to each service individually

By accessing services via a federated enterprise identity, not only the user experience is improved, but also Enterprise compliance controls of user access are easier to satisfy, ensuring only valid identities may access cloud services.

4.11.2 Goal or Desired Outcome

A user is able to access resource within their enterprise environment or within a cloud deployment using a single identity. Once authenticated, the user access to the application is authorized and audited by the cloud application

4.11.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ Federated Identity Mgmt. (FIM) ○ General Authentication ○ Single Sign-On (SSO) • Secondary ○ None	**Featured Deployment and Service Models:** • Cloud Deployment Models ○ None featured • Service Models ○ None featured
Actors: • Subscriber Enterprise Application Administrator • Subscriber Enterprise User	**Systems:** • Cloud Identity Mgmt. System, which includes support for: ○ Cloud Application Administration Service ○ Cloud Application Identity Federation Service ○ Cloud Application Authorization Service
Notable Services: • Enterprise Identity Provider • Cloud Provider Authentication Service	

- Enterprise Account and Attribute Service (identity transformation)

Dependencies:

- Prior to Authentication, the Enterprise (tenant) Application Administrator has set up the Enterprise User's account at the cloud provider with appropriate entitlements for the Cloud Application out of band OR just-in-time provisioning takes care of that
- The federated trust relationship between the Cloud Provider (hosting the Cloud Application) and the Enterprise's Identity Provider was previously set by the Subscriber Enterprise's Application Administrator.

Assumptions:

- The use case does not cover the identity proofing process of the Enterprise's Cloud Provider Account Owners. The process is happening out of band to the use case.

4.11.4 Process Flow

1. The Subscriber Enterprise's User accesses a cloud hosted application's URL with their browser
2. The Subscriber Enterprise's User is redirected to the Enterprise's Identity Provider (IdP) for authentication by the Cloud Provider's Application
3. Based on policy, the authentication process between the Enterprise User providing credentials, the Cloud Provider's Application Identity Federation and Authorization Service and the Enterprise IdP may facilitate Single Sign-On (SSO) leveraging one of the following
   3.1. The existing authentication session
   3.2. Re-authentication of the user, prompting the user to re-authenticate using plain step up authentication scheme (requiring multi factor authentication).
4. The Enterprise IdP may perform account mapping functions and translate the enterprise identity to an identity the cloud provider's service can accept.
5. Upon successful authentication process, the Subscriber Enterprise's User is redirected back to the cloud provider and is able to access the desired cloud hosted application.

4.12 Use Case 12: Consumer Cloud Identity Management, Single Sign-On (SSO) and Authentication

4.12.1 Description / User Story

With the broadening of services offered in the cloud, the identity management and authentication of users to the services is under pressure to be decoupled from the cloud services themselves. From a user perspective, Users subscribing to an array of cloud services expect and need to have an interoperable identity that would be used to obtain different services from different providers.

From a cloud provider perspective, being able to interoperate with identities the user already have, helps to attract new customers, and would simplify the identity management overhead of the service provider. A cloud centric authentication service, using federated identity standards such as SAML and WS-Federation, is a key component of a streamlined user experience and obtaining trust in the cloud

4.12.2 Goal or Desired Outcome

A user (or cloud consumer) is able to access multiple SaaS applications using a single identity. Once authenticated using the Identity Provider, the user access to different SaaS provider applications does not require the user to re-authenticate to each application individually

4.12.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ Federated Identity Mgmt. (FIM) ○ General Authentication ○ Single Sign-On (SSO) • Secondary ○ None	**Featured Deployment and Service Models**: • Cloud Deployment Models ○ Public ○ Community • Service Models ○ Software-as-a-Service (SaaS)
Actors: • Subscriber SaaS Application User • Subscriber SaaS Provider Administrator	**Systems:** • Cloud Identity Mgmt. System, which includes management support for: ○ SaaS Applications • External Identity Provider (Service)
Notable Services: • Cloud Provider Identity Federation Service • Cloud Provider Attribute Management Service (identity transformation)	
Dependencies: • The federated trust relationship between the SaaS application and the identity provider was previously set by the Cloud tenant Administrator. • The user accessing the service is already registered and enrolled with the Identity Provider of choice.	
Assumptions: • User enrollment to a SaaS application is out of scope for the use case. The user enrollment process can be done using a registration process out of band, or using just-in-time provisioning.	

4.12.4 Process Flow

1. The Subscriber’s SaaS Application User accesses the URL for the Cloud SaaS Application with their browser.
2. The Subscriber’s SaaS Application User is redirected to an External Identity Provider service
3. The External Identity Provider prompts the Subscriber’s SaaS Application User for their credentials.
   3.1. This process may advantage SSO using a browser cookie or require the user to re-authenticate using plain password or multifactor authentication.
4. Upon successful completion of the authentication process, the user’s identity is mapped or transformed to one that is recognized by the cloud provider hosting the SaaS application.

5. The Subscriber SaaS Application User is redirected to the Cloud SaaS Application which they are now able to access with the transformed identity.

4.13 Use Case 13: Transaction Validation & Signing in the Cloud

4.13.1 Description / User Story

As business applications and services are moving from the internal perimeter and to the cloud, there is a need in transaction integrity and validation for cloud transactions.

Electronic and digital signing are associated traditionally with an endpoint controlled secret key, such as a One-Time Password (OTP) token (facilitating single use signing), or by using a previously established private key stored on the PC or in some secure container (such as a smartcard).

Users and systems that consume cloud services present themselves in different form factors and end points, including, but not limited to traditional PCs and tablets as well as mobile devices and smart phones.

As access to cloud hosted resources and applications increase, so does the need to provide a transaction validation and signing for business applications that flexible to use with different end point form factors and may be delivered as a service.

4.13.2 Goal or Desired Outcome

Users are able to perform transaction and document signing in the cloud using a trusted signing service that manages their signing keys.

4.13.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ General Identity Mgmt. ○ General Authentication • Secondary ○ Audit and Compliance	**Featured Deployment and Service Models:** • Cloud Deployment Models ○ Public • Service Models ○ None featured
Actors: • Subscriber Company User	**Systems:** ○ External Identity Provider
Notable Services: • Cloud Provider Authentication Service • Cloud Provider Signing Service ○ Supports Transaction Signing, Key Registration and Enrollment • Cloud Provider Auditing Service ○ Supports Transaction-level Auditing	

Dependencies:

- Authentication - be able to authenticate users (a person), services (or systems) and organizations using different levels of assurance and authentication schemes (password, certificate, hardware tokens, out of band, biometric).
- The Cloud Provider Signing Service has the ability to:
    - Transaction Signing – sign transactions by binding identity, transaction information and a signature using compliant certification levels such as common criteria or FIPS certification.
    - Transaction Auditing – record signing events in a tamper evident/tamper resistance transaction log.

Assumptions:

- Use of standardized encryption and signing techniques for message / transaction-level signing that includes binding of verifiable identities.
- The signing entity have gone through an identity proofing process out-of-band, and enrolled the user for the service - established and generated a signing key for that user and created a binding between that key and an authentication scheme for the user.
- The methods / techniques used to sign and bind it to the document are not detailed in this use case.

4.13.4 Process Flow

1. The Subscriber's Company's User accesses an application that requires document signing.
2. The application access the Cloud Provider's Signing Service (browser re-direction or active connection to the signing service).
3. The Cloud Provider's Signing Service works with the Cloud Provider's Authentication Service to authenticate the user at the appropriate level of assurance (preferably by using a multi-factor authentication scheme) perhaps by:
    3.1. Prompting the user for their credentials (direct authentication to the cloud provider).
    3.2. Redirects the user to the user is redirected to their chose (External) Identity Provider
4. Once the Subscriber Company's User credentials are validated successfully, the Identity Provider (IdP) redirects the user to the Cloud Provider's Signing Service.
5. The Cloud Provider's Signing Service processes the signing request generating the signature for the transaction / document and signs the document and returns it to the requesting application.
    5.1. Note that the signature can by bound the document using various techniques; such as embedding in the document itself or signing a container or transaction that includes the document when it is returned to the application.
6. Upon document signing, the Cloud Provider's Auditing Service records (logs) for audits the signing operation and signature along with any relevant identities.

4.14 Use Case 14: Enterprise Purchasing from a Public Cloud

4.14.1 Description / User Story

This use case is concerned with enterprise users from company A accessing a supplier's (company B) online shop hosted in the public cloud. Employees of company A log on to internal

Supplier Relationship Management (SRM) system and can browse a catalogue of suppliers and order goods from there.

Sales orders in the supplier's online shop must be approved by the manager of the employee who placed the order. Once the sales order is approved, a new purchase order is created and processed in the internal supplier's Customer Relationship Management (CRM) System.

Company A employees with special privileges (e.g. controllers) can export order data from the supplier's online shop and CRM system and the analyze the datasets in an Business Intelligence (BI) system which is also hosted in the public cloud.

Figure 1 - Enterprise Purchasing Use Case Overview, provides an overview of all three parts that comprise the enterprise purchasing use case:

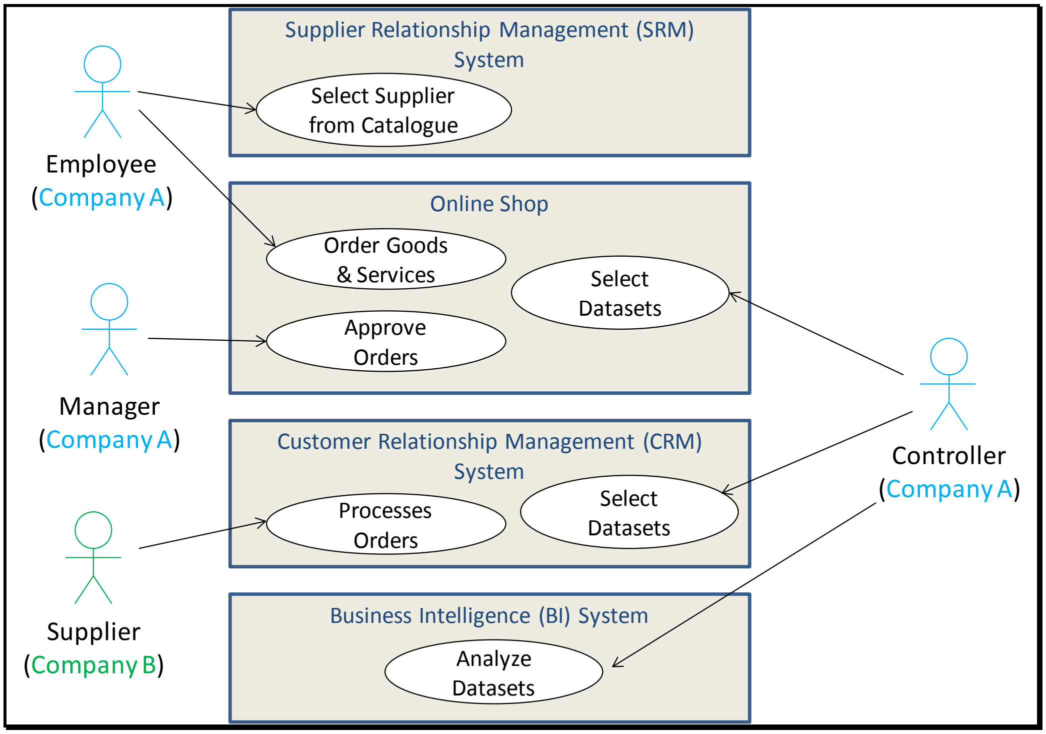


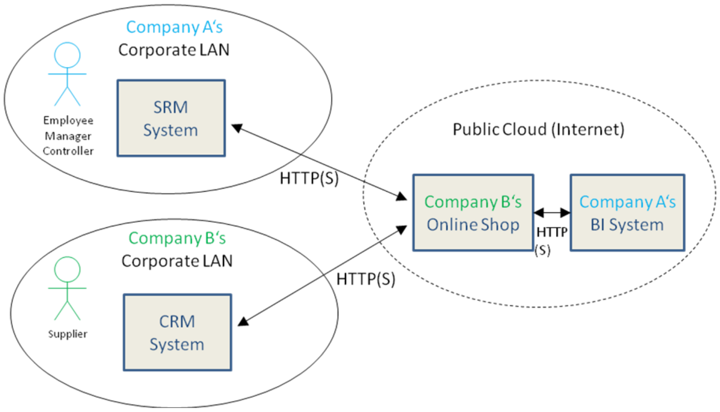
FIGURE 1 - ENTERPRISE PURCHASING USE CASE OVERVIEW

4.14.2 Goal or Desired Outcome

- Enable Single Sign-on (SSO) between enterprise (on-premise) and cloud-based (on-demand) applications for employees accessing the supplier's online shop via the internal SRM system. This applies to classical front-channel access (i.e. Web Browser-based) as well as back-channel communication (i.e. Application-to-Application (A2A) integration between the SRM system and the online shop) perhaps using RESTful APIs.
- Ideally no directory synchronization or user account provisioning between the internal (on-premise) and external/cloud (on-demand) systems to enable SSO.

- SSO that supports RESTful APIs provided by the systems in the public cloud should use a standardized token format and protocol binding
- (Semi) automated trust setup between on-premise and on-demand systems.

4.14.3 Notable Categorizations and Aspects

<table>
<tr><td><b>Categories Covered:</b>
• Primary
○ Infrastructure identity Establishment
○ Single Sign-on (SSO)
• Secondary
○ Authorization
○ Security Tokens</td><td><b>Featured Deployment and Service Models:</b>
• Cloud Deployment Models
○ Public
• Service Models
○ Software-as-a-Service (SaaS)</td></tr>
<tr><td><b>Actors:</b>
• Subscriber Company Actors:
• Company A Employee
• Company A Employee Manager
• Company A Controller
• Company B Supplier</td><td><b>Systems:</b>
• Enterprise Supplier Relationship Mgmt. (SRM) System
○ in Company A's internal/corporate LAN
• Enterprise Customer Relationship Mgmt. (CRM) System
○ in Company B's internal/corporate LAN
• Company B's online shop
○ in the Public Cloud
• Company A's Business Intelligence (BI) System
○ in the Public Cloud


Company A's
Corporate LAN
Employee
Manager
Controller
SRM
System
HTTP(S)
Public Cloud (Internet)
Company B's
Online Shop
HTTP
(S)
Company A's
BI System
Company B's
Corporate LAN
Supplier
CRM
System
HTTP(S)

</td></tr>
<tr><td colspan="2"><b>Notable Services:</b>
• Enterprise Identity Provider Service
○ Central authentication system hosted in company A's internal network. Issues a security token that can be used for SSO to the supplier's online shop. Manages all user-related data like credentials and roles.
• Cloud Provider's Identity Provider Service
○ Token issuer operated by the Public Cloud provider that issues security tokens to enable SSO</td></tr>
</table>

between cloud and on-premise systems.

- Cloud Providers Identity Mgmt. Services
  - Supports cloud applications in validating and authenticating security tokens issued by identity providers.

Dependencies:

- Transport- and/or message-level integrity and encryption.
- Standardized token formats and protocol bindings that support SSO for RESTful APIs.

Assumptions:

- Company A's Employee authenticates at the internal Enterprise IdP before accessing the SRM system and the supplier's (Company B's) online shop.
- Company B's online shop "understands" Company A's claims semantics (i.e. roles/functions like "employee", "manager" and "controller") to authorize user actions in the shop (i.e. create a sales order, approve a sales order, export sales orders).
- Company B's online shop can authenticate and log-on Company A users even without an existing user account in the Cloud.
  - If an account has been provisioned for the user to the Cloud, the Enterprise Identity Provider should maintain the user mapping between the corporate and cloud user account.
- Trust has been established between Company A's and Company B's applications (e.g. Company B's online shop and CRM System, Company A's SRM System and Identity Provider).
- The cloud provider supports RESTful APIs for all their applications and services.

4.14.4 Process Flow

The process flow for this use case is divided into three parts:

- **Part 1**: Covers the order and approval process of a new sales order (on-premise to on-demand SSO)
- **Part 2**: Addresses the creation of the purchase order (on-demand to on-premise SSO)
- **Part 3**: Exhibits the need to support on-demand SSO to assist in analyzing data (e.g. Business Intelligence) from different source locations (deployments).

4.14.4.1 Part 1 – Order and Approval

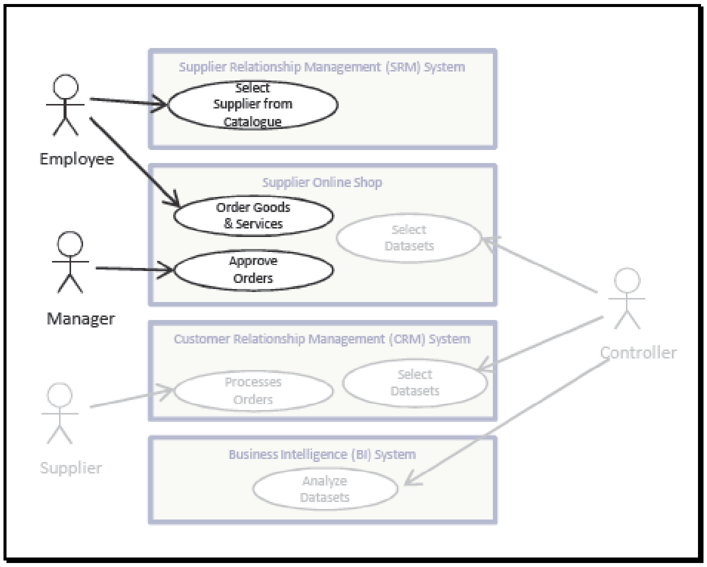

Supplier Relationship Management (SRM) System
Select Supplier from Catalogue
Employee
Supplier Online Shop
Order Goods & Services
Select Datasets
Approve Orders
Manager
Controller
Customer Relationship Management (CRM) System
Processes Orders
Select Datasets
Supplier
Business Intelligence (BI) System
Analyze Datasets

FIGURE 2 – EMPLOYEE ORDER / MANAGER APPROVAL PROCESS FLOW

1. Company A’s Employee authenticates to the Enterprise’s Identity Provider Service to obtain access to Company A’s Supplier Relationship Mgmt. (SRM) system to select a supplier (Company B) from the catalogue to purchase goods

2. The SRM system forwards employee‘s web browser to Company B’s (the supplier‘s) online shop (a cloud hosted application) in the Public Cloud.

    2.1. Company A’s Employee uses front-channel SSO to authenticate.

3. Company A’s Employee selects goods and services from the Company B’s online shop catalogue and places a sales order in the online shop.

4. Company A’s Employee Manager receives an email notification about the new sales order and logs into Company B’s (the supplier’s) online shop via SSO.

5. Company A’s Employee’s Manager approves the new order in the online shop.

4.14.4.2 Part 2 – Purchase Order Creation

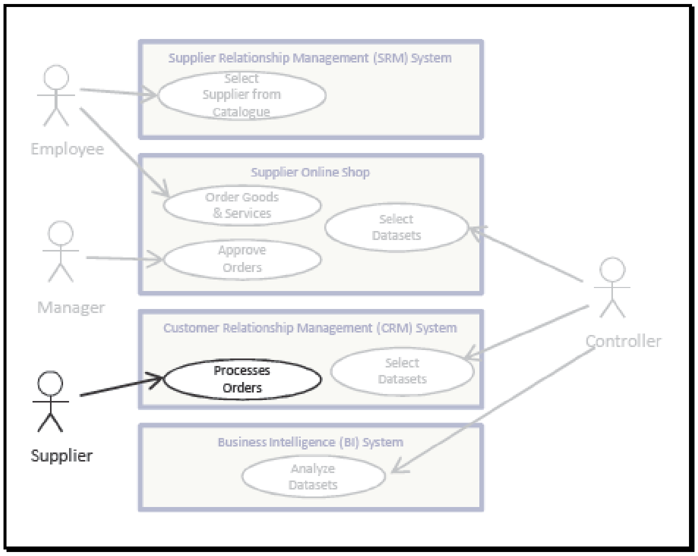

Supplier Relationship Management (SRM) System
Select Supplier from Catalogue
Employee
Supplier Online Shop
Order Goods & Services
Select Datasets
Approve Orders
Manager
Controller
Customer Relationship Management (CRM) System
Processes Orders
Select Datasets
Supplier
Business Intelligence (BI) System
Analyze Datasets

FIGURE 3 - SUPPLIER PROCESS ORDER FLOW

6. Company B's online shop application creates a purchase order in the Company B's Customer Relationship Mgmt. (CRM) system.

   6.1. Company B's Supplier gets notification of the purchase order.

7. Company B's Supplier processes the purchase order in the CRM system and an email notification is sent to Company A's Employee about the updated status

4.14.4.3 Part 3 – Business Intelligence and Analytics

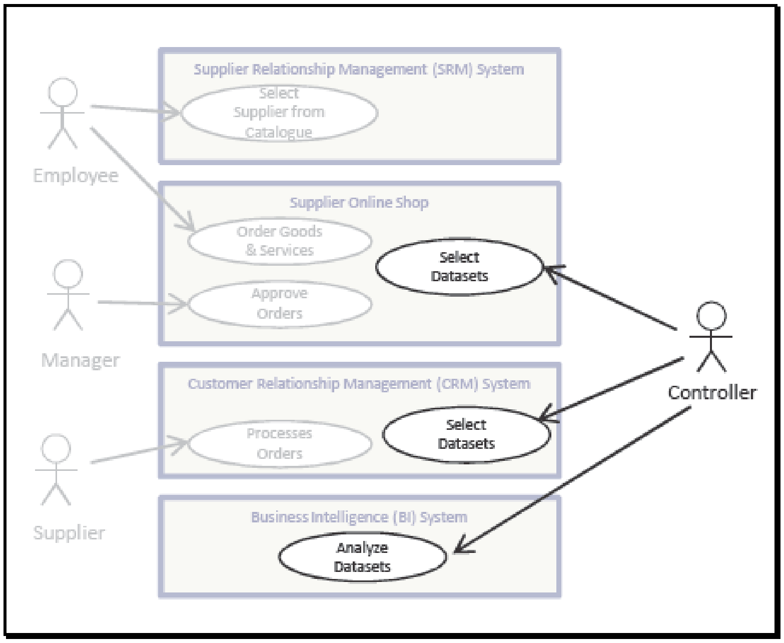

Supplier Relationship Management (SRM) System
Select Supplier from Catalogue
Employee
Supplier Online Shop
Order Goods & Services
Select Datasets
Approve Orders
Manager
Controller
Customer Relationship Management (CRM) System
Processes Orders
Select Datasets
Supplier
Business Intelligence (BI) System
Analyze Datasets

FIGURE 4 - CONTROLLER PROCESS FLOW

8. Company A’s Controller of company A authenticates via SSO at the supplier online shop and selects all orders created by employees in Company A in the last month to analyze the purchases over this time
9. Company B’s online shop retrieves additional data from Company B’s CRM system regarding the selected orders and uploads the dataset to Company A’s Business Intelligence (BI) system hosted in the public cloud.
10. Company A’s Controller authenticates via SSO to Company A‘s Business Intelligence (BI) system hosted in the public cloud and analyzes the uploaded datasets.

4.15 Use Case 15: Access to Enterprise’s Workforce Applications Hosted in Cloud

4.15.1 Description / User Story

The Enterprise is making certain productivity applications, such as electronic mail (or email) and Customer Relationship Management (CRM) available to its workforce via the cloud.

4.15.2 Goal or Desired Outcome

Employee’s authentication status conveyed from enterprise to public SaaS provider so that appropriate access privileges can be granted to access requests – for both browser-based and API-based applications.

A desired outcome would be OASIS developing one or more profiles or specifications that build on existing standards (e.g. SAML, OAuth) or creating additional open standards to address technical gaps identified by this use case.

4.15.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ Federated Identity Mgmt. (FIM) • Secondary ○ General Authentication ○ Authorization	**Featured Deployment and Service Models:** • Cloud Deployment Models ○ None featured • Service Models ○ Software-as-a-Service (SaaS)
Actors: • Enterprise Employee	**Systems:** • Enterprise Identity Mgmt. System • Identity Provider Service • e.g. a Kerberos Identity Provider Service
Notable Services: • Cloud CRM Service • Cloud Electronic Mail Service • Enterprise-KDC	

- Cloud-KDC
- Enterprise-run Service

Dependencies:

- None

Assumptions:

- The Enterprise is the authoritative source of identity for its workforce and that this authoritative source (i.e. the directory) may be on-premise or itself in the cloud.
- Business relationship with cloud provider has been established to permit seamless authentication and authorization to resources.
- ***Infrastructure Trust Establishment***: (in this case between the enterprise/user and the Kerberos Authentication Service in the Cloud
- ***General identity management***:
    - *Infrastructure identity management*: Kerberos has been and is currently being used as a popular authentication mechanism within virtualized environments. In most cases, the deployment scenario demands distinct Kerberos identities, in order to allow separation of the logical resources as well as for audit requirements.
- **Authentication**: The Kerberos Authentication Service in the Cloud can be narrowly defined as an authentication service that operates one or more Kerberos KDCs in the cloud and providing a web-layer API for Kerberos Clients and Kerberos Service Principals (i.e. SPs). An important requirement is the ability of an end-user to perform SSO to a known (participating) SP after authenticating to appropriate Cloud-KDC.
- **Authorization**: A crucial part of achieving cross-provider consistent security quality is to provide a common authorization semantics that can be evaluated (e.g. By a PDP) and enforced (e.g. by a PEP). Currently in the IETF there is a new draft proposing a generalized Kerberos attribute set.
- **Account and attribute management**: This use-case requires a secure method to establish new accounts, manage existing accounts and to manage attributes related to an account in a consistent manner across organization (e.g. cross-enterprise).
- **Provisioning**: This use-case requires a method to provision accounts into a Kerberos Authentication Service in the Cloud. This includes provisioning the credentials (eg. master-key(s)) at the Client and Cloud-KDC, cipher-types, as well as other operating policies. Such a provision system should be administered by a legitimate Administrator operating under the jurisdiction of the Enterprise or the Cloud-KDC.
- **Security Tokens**: Although the Kerberos ticket is a well-known data structure and well deployed in the Enterprise, in order to interoperate with non-Kerberos services in the wider Internet, we anticipate the need of a token-translation to occur. This could be either as part of the Cloud-KDC function or as a separate token translation service.

4.15.4 Process Flow

4.15.4.1 General Scenario

1. Employee logs-in to Enterprise's Identity Management (IM) System.
2. Employee is able to seamlessly access subscribed cloud hosted services such as electronic mail (email) or Customer Relationship Mgmt. (CRM) Services & related cloud based resources which are maintained at the SaaS provider.

- This could be accomplished directly via a SaaS-hosted browser application or an enterprise application using interfaces or APIs made available by the SaaS provider.

4.15.4.2 Kerberos Scenarios

4.15.4.3 Description / User Story

There is a strong desire on the part of many Enterprises to expand their existing authentication mechanisms and protocols (such Kerberos) for authentication to the cloud.

Enterprises that employ Kerberos would like to issue Kerberos tokens (tickets) to their employees to perform single-sign-on (SSO) to affiliated services outside the enterprise. Similarly, other organizations wish to allow their consumers/customers to access resources/services offered by the organization using a strong authentication protocol, preferably one which is compatible to their internal authentication infrastructure.

This dual need could be addressed by the deployment of a Kerberos authentication and authorization Service in the Cloud (Cloud-Kerberos). That is, an authentication service that operates one or more Kerberos KDCs in the cloud and providing either a hosted infrastructure-as-a-service to Enterprises or to a trusted third-party IdP. Another means would be for the cloudprovider to be Kerberos aware and be able to map Kerberos tokens into ones the cloud provider uses.

The former approach, would require several technical issues to be addressed. These include development of global identities for Kerberos (real and pseudonymous), a standard web-layer API for authentication services, Enterprise-to-Cloud trust establishment, a global authorization structure, provisioning of users and credentials to the cloud, and others.

4.15.4.4 Scenario 1: Enterprise Employee Outbound

1. Employee obtains Kerberos Ticket Granting Ticket (TGT) from Enterprise KDC (internal).
2. Employee presents TGT in an outbound connection to the Cloud-KDC (external Kerberos-IdP).
3. Cloud-KDC returns a Kerberos service-ticket or equivalent (e.g. OAuth2.0 Access Token)
4. Employee presents the service-ticket to an external Service Provider.
5. Employee obtains service or resource from external Service Provider.

4.15.4.5 Scenario 2: Consumer/customer (Inbound into Enterprise-run service)

1. Consumer obtains a Kerberos Ticket Granting Ticket (TGT) from the Cloud-KDC (external Kerberos IdP).
2. Consumer presents TGT to the out-facing Enterprise-KDC.
3. Enterprise-KDC returns a Kerberos service-ticket or equivalent (e.g. OAuth2.0 Access Token)
4. Consumer presents the service-ticket to desired Enterprise-run service.
5. Consumer obtains service or resource from Enterprise-run service.

4.16 Use Case 16: Offload Identity Management to External Business Entity

4.16.1 Description / User Story

The Enterprise is making certain applications available to either the employees of its customers & business partners, or consumers, and wants to avoid directly creating and managing the accounts (identities) for those users – instead pushing the management of those user accounts and credentials to the relevant external business entity.

This use case can be seen as being related to use case #15 "Access to Enterprise's Workforce Applications hosted in Cloud", but instead of the Enterprise's employees using Workforce SaaS applications hosted at a SaaS provider the Enterprise's Customers wishes to extend access to additional SaaS applications to other user types.

4.16.1.1 Institutional Customers

An enterprise has institutional customers requesting that their employees have seamless access (i.e. SSO) into the enterprise's customer-facing applications (e.g. employees of an institutional customer being able to access their 401K, Benefits, Payroll, etc.). The fundamental business & trust relationship is between the enterprise and the customer – that between the enterprise and the employees is secondary.

4.16.1.2 Business Partner Employees

The Enterprise is making certain applications available to its business partners for the purposes of collaboration. The fundamental business & trust relationship is between the enterprise and the business partner – that between the enterprise and the employees is secondary.

4.16.1.3 Consumers

An enterprise wants to be able to accept identities from public Social Networks, such as FaceBook or Twitter, to enable access into the enterprise's consumer-facing applications. This sub-case is distinguished by both a likely more dynamic trust model between Enterprise and the Social Networks, and the likely need for explicit user consent before any identity attributes are shared.

4.16.2 Goal or Desired Outcome

Authentication status of end-user (employee of business partner or customer, or consumer) conveyed from appropriate identity provider to enterprise so that enterprise can grant appropriate privileges to access requests – for both browser-based and API-based applications.

4.16.3 Notable Categorizations and Aspects

Categories Covered:	**Featured Deployment and Service Models:**

• Primary ○ Federated Identity Mgmt. (FIM) • Secondary ○ General Authentication ○ Authorization ○ General Account and Attribute Mgmt.	• Cloud Deployment Models ○ None featured • Service Models ○ Software-as-a-Service (SaaS)
Actors: • Enterprise • Business Partner/Customer • Employee/consumer • Social Network Provider	**Systems:** • None
Notable Services: • Identity Provider Services	
Dependencies: • Federated Identity Management (FIM)	
Assumptions: • Trust established between enterprise, the cloud provider and its business partners • Enterprise and its business partners have agreed upon approved authorization mechanisms and identity providers.	

4.16.4 Process Flow

1. An Enterprises' Institutional Customers, Business Partner Employees, or Consumers log-in to the approved Identity Provider for their application. The identity provider could be managed by the Enterprise itself, by the Business Partner or be managed by a Consumer's preferred Social Network Provider (e.g. FaceBook or Google).

2. The Business Partner or Institutional Customer or Social Network's Identity Provider asserts the identity attributes of the User to the Enterprise.

3. Employees or consumers are able to access relevant services & resources maintained at Enterprise (perhaps via dedicated client, hosted or browser-based applications) regardless of location of Identity Provider.

4.17 Use Case 17: Per Tenant Identity Provider Configuration

4.17.1 Description / User Story

Multi-tenant service providers, whether they are SaaS, PaaS, or IaaS vendors, benefit from quick and easy addition of new customers – anyone with a credit card can add themselves on demand. However, to benefit from federated authentication, SSO, and other mechanisms that can improve security for their users they need to configure how their users can authenticate to the system, where and what kind of IdP they use, exchange meta-data, etc. Currently this is commonly done by the administrator via web forms that are unique to each service. As adoption of cloud services increases, this will become a significant management burden.

4.17.2 Goal or Desired Outcome

A tenant can quickly and securely manage their use of many cloud services using automated tools rather than navigating and manually configuring each service individually.

4.17.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ Infrastructure Identity Establishment ○ Federated Identity Mgmt. (FIM) • Secondary ○ None	**Featured Deployment and Service Models:** • Cloud Deployment Models ○ None featured • Service Models ○ None featured
Actors: • Tenant Administrator • Multi-tenant Service Provider • Identity Provider	**Systems:** • None
Notable Services: • Cloud Applications and Services • Cloud Identity Provider Services • Cloud Attribute Services • Identity Provider Discovery services	
Dependencies: • None	
Assumptions: • Wide-spread adoption of federated authentication due to rapid adoption of cloud computing. • The "Categories Covered" highlights the key aspects of this use case. It is assumed that all APIs and protocols used to accomplish the configuration would be follow appropriate General Identity Management, Authentication, Authorization, and Audit principles.	

4.17.4 Process Flow

1. A departmental manager in an enterprise (a tenant administrator) wants to configure all of the SaaS applications in use by that department to authenticate users via the enterprise Identity provider.
2. Using an automated tool to manage her SaaS usage, she enters the Identity Provider information once.

3. The tool contacts the Identity Provider and each SaaS application and uses standard protocols to communicate the configuration.

4.18 Use Case 18: Delegated Identity Provider Configuration

4.18.1 Description / User Story

Enterprises are outsourcing more of their applications and management of their IT infrastructure – including their identity provider services – to managed service providers or Identity-as-a-Service vendors. This results in a situation where an enterprise administrator which owns the business relationship with the service provider (the tenant administrator) does not manage the identity provider service. The identity provider service is controlled and managed by another company (i.e. an Identity Provider Administrator). This becomes a significant management burden when the tenant administrator needs to manage the identity services configuration (such as the exchange of metadata) between the identity provider and many cloud services.

4.18.2 Goal or Desired Outcome

The tenant administrator should be able to delegate access to their identity services configuration within a multi-tenant cloud service to the identity provider service. The identity provider service should be able to manage configuration issues such as meta-data exchange to all connected cloud services on behalf of a tenant. This should not require the identity provider to had access to the tenant administrator's authentication credentials.

4.18.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ Infrastructure Identity Establishment • Secondary ○ General Authentication ○ Authorization ○ Account & Attribute Mgmt.	**Featured Deployment and Service Models:** • Cloud Deployment Models ○ None featured • Service Models ○ None featured
Actors: • Tenant Administrator • Identity Provider Service	**Systems:** • Cloud Service Provider (Multi-tenant)
Notable Services: • Cloud Applications and Services • Cloud Identity Provider Services • Cloud Attribute Services	

Dependencies: • This use case depends on use case #17 “Per Tenant Identity Provider Configuration” as a basis.
Assumptions: • The “Categories Covered” section highlights the key aspects of this use case. It is assumed that all APIs and protocols used to accomplish the configuration would be follow appropriate General Identity Management, Account management, and Audit principles.

4.18.4 Process Flow

1. A tenant administrator pulls out a credit card and signs up for a new cloud services for her users. Her identity services are provided by a third party.
2. She notifies the identity provider that she wants her users to have access to the new services.
3. The identity provider can exchange whatever configuration and meta-data is required with each new service on behalf of the tenant administrator without authenticating to each service as her.

4.19 Use Case 19: Auditing Access to Company Confidential Videos in Public Cloud

4.19.1 Description / User Story

A media company wishes to store its confidential training videos in a Public Cloud that provides low-cost storage. These videos can be downloaded by valid employees during specified training periods.

Certain company managers and developers are permitted to upload, update or delete videos. The company’s security auditors perform monthly audits to verify accesses to these videos are by valid,
current employees only and that their access policies have been enforced.

The media company's security auditors need the ability to compile all applicable audit data (on its video accesses) monthly into a report that they can move to their secure cloud storage area and perhaps be able to export it back to their enterprise securely.

4.19.2 Goal or Desired Outcome

The media company is able to use public cloud storage for managing its confidential training videos while preserving enforcement of their security policies and existing role-based processes.

That the company is able to extract audit reports from the cloud provider that provide a means to show clear compliance to those policies including clear identification of all employees and their actions.

4.19.3 Notable Categorizations and Aspects

Categories Covered:	**Featured Deployment and Service Models:**
• Primary ○ Audit and Compliance • Secondary ○ Single Sign-On (SSO) ○ Authorization	• Cloud Deployment Models ○ Public • Service Models ○ Infrastructure-as-a-Service (IaaS)
Actors:	**Systems:**
• Company Security Engineer • Company Human Resource Manager • Company Employee • Company Security Auditor • Company Compliance Officer	• None

Notable Services:

- Public Cloud Management Platform:
    - Single Sign-On (SSO) – User Authentication to Public Cloud provides credentials needed to Manage/Access Cloud Storage Services.
    - Access Control Services – Manage Roles and Security Policies
        - Granular to the individual Stored Item (e.g. each Company Video) or Group/Container of Items (e.g. Company Training Videos Folder).
    - Cloud Storage Services – Manage Cloud Content (e.g. Upload, Download, Delete, Tag, View, etc.) such as company videos and enforce company's security policies.

Dependencies:

- Endpoint security for user authentication.
- Endpoint transaction security for storage services.

Assumptions:

- Company has established an account with the public cloud service provider along with any "root" trust credentials to further administer more granular (service or resource level) security policies.
- Access Control: Company is able to manage its security policies and associate them to cloud enabled processes (i.e. define roles with permissions that can be assigned to employees based upon their job role). That employee identities
- Consistent Audit Record: Cloud provider's infrastructure and management services produce auditable records against all cloud storage actions. That these records can be compiled into a consistent auditable trail. Considerations Include:
    - The ability to identify unique users/accounts, applications/services and resources (e.g. network, storage) that were involved in completing a cloud (storage) action.
    - The ability to correlate cloud (storage) transactions across infrastructure boundaries (i.e. identities and authentications are preserved).
    - Identify Security Policy Enforcement/Decisions that produce a clear result.
    - Consistent Timestamp
- Geography: Cloud provider and company are in the same geography and subject to the same governance rules/policies.

- Data: Video format, encryption and upload protocols are not considered.
- Storage: Low-level storage actions are audited (including archiving, redundancy, permanent deletion).

4.19.4 Process Flow

1. A security engineer in the media company uses Singe Sign-On (SSO) to the cloud provider to access Cloud Storage Services and creates a Confidential Cloud Storage Folder that will hold company confidential employee training videos.
2. The security engineer then defines employee roles and security policies for accessing confidential videos (consistent with the company's established policies and processes) and associates them to all content that will be assigned to that Confidential Cloud Storage Folder.
3. The security engineer logs off using Single Sign-Off.
4. The security engineer's logon/logoff, Cloud Storage Services accesses, creation of a Confidential Cloud Storage Folder and definition of the folder's security policies (along with authorization decisions that enabled folder creation and policy definition) are recorded by the public cloud provider.
5. A human resource manager of the media company uses SSO to the cloud provider to access Cloud Storage Services and uploads a confidential employee training video to the Confidential Cloud Storage Folder the security engineer created. The training video is assigned a unique resource name and/or identifier along with a human readable name.
6. The human resource manager logs off using Single Sign-Off.
7. The human resource manager's logon/logoff, Cloud Storage Services accesses and video upload to the Confidential Cloud Storage Folder (along with authorization decisions that enabled video upload) are recorded by the public cloud provider.
8. A new employee of the media company needs to view the confidential training video within the first month of their employment.
9. The new employee Single Sign-On (SSO) to the cloud provider and is presented with a portal that displays the company's confidential training video (using the human readable name).
10. The new employee "plays" the video and watches it from start to finish.
11. The new employee logs off using Single Sign-Off.
12. The new employee's logon/logoff, Cloud Storage Services accesses and video upload to the Confidential Cloud Storage Folder (along with authorization decisions that enabled video upload) are recorded by the public cloud provider.
13. The media company's corporate Compliance Officer (CO) uses the cloud provider's SSO service to logon and access the Cloud Storage Services.
14. The CO is able to verify that the new employee completed watching the confidential employee training video in the time allotted. This is accomplished by being able to retrieve an auditable record that uniquely identifies both the new employee and resource (video), as well as the access times and duration of the resource using a consistent (cloud provider supplied) timestamp.
15. The CO logs off using Single Sign-Off.
16. The CO's logon/logoff, Cloud Storage Services accesses and access of audit records for employees accesses to the Confidential Cloud Storage Folder (along with authorization decisions that enabled this type of audit) are recorded by the public cloud provider.

17. The media company needs to perform a quarterly audit of all confidential video accesses (successful or not) to search for any anomalies. Therefore, the company's Security Auditor uses the cloud provider's SSO to logon and access the Cloud Storage Services and retrieve a report of all access attempts on the Confidential Cloud Storage Folder.
18. The Company Security Auditor logs off using Single Sign-Off.
19. The Company Security Auditor's logon/logoff, Cloud Storage Services accesses and report generation are all recorded by the public cloud provider.

4.20 Use Case 20: Government Provisioning of Cloud Services

4.20.1 Description / User Story

A vendor offering the provisioning of cloud services (i.e. using any "as-a-Service" types) to government agency operatives offers two online service on-boarding options:

1) through a website to provision simpler, smaller ad hoc cloud services, similar to the retail public cloud portals and
2) via a B2B (machine based) Web Services call through a common front-end portal or provision larger, more complex services.

Using a web browser, a government agency operative (not necessarily an employee and could be a contracted outsourced vendor operative accessing remotely from a different realm to the agency) logs on to a web page that offers online tools to configure and provision the environment they need. They define the configuration of the services they need, and once processed by the cloud provider, confirmed online in real time and captured in the cloud provider's configuration management database application.

The Web Services call follows an appropriate programmatic process to achieve the same result, but in addition, the confirmation is captured in the government agency's/outsourced vendor's configuration management database.

The online management processes (provisioning and de-provisioning history, activity and access monitoring, reporting, billing etc) is done via either the same browser based customer portal that offers the provisioning, or a separate one, depending on the vendor's approach.

In order for the service to operate to high standards of security, confidentiality and integrity, the key identity management requirements will be Identity Proofing, Authentication and Authorization, and Role Management for delegated functions and separation of duties. For external access to the cloud based provisioning service, these functions are the responsibility of the agency. For access required from within the service, these functions are the responsibility of the vendor. The online management processes capture the activities of both external and internal activity related to the service.

4.20.2 Goal or Desired Outcome

Authorized personnel will be granted access and appropriate privileges to configure and provision the service. All access requests will be verified to ensure that the user is who they say they are, and have a legitimate requirement for access to the service.

4.20.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ General Authentication • Secondary ○ Authorization ○ Audit and Compliance	**Featured Deployment and Service Models:** • Cloud Deployment Models ○ None featured • Service Models ○ None featured
Actors: • Cloud vendor & their OEMs etc • Government agency • Government agency employee • Government agency outsource provider/third party support org	**Systems:** • None
Notable Services: • Cloud Applications and Services • Either Cloud or off-cloud (centralized) Identity Provider Services • Either Cloud or off-cloud (centralized) logon Services • Cloud Access/Privilege Management Services • Cloud Attribute Services	
Dependencies: For the B2B web services call, a commonly agreed API and assertion method will be required for all agencies and all suppliers	
Assumptions: • Contractual relationship and SLA already established and operating between government agency and cloud vendor • Contractual relationship and SLA already established and operating between government agency and its outsource provider/third party support (if applicable) • The cloud provider supports authorization from both browser-based and API (Web Service) based applications.	

4.20.4 Process Flow

1 Example: A member of the government agency team logs on to a web page that offers online tools to configure and provision the environment they need.

2 They define the configuration of the services they need, choosing and confirming from a menu of pre-configured capacity, feature and function templates and pre-configured Service Level templates, and optional blank templates for custom requirements, and entering enter cost centre and billing authorization codes, at the check-out facility.

3 The activity is captured in the applicable configuration management databases and confirmed online in real time.

4 Later, at some scheduled interval or as required for the purposes of SLA compliance, security and privacy, the agency's audit and compliance department accesses the online management processes (provisioning and de-provisioning history, activity and access monitoring, reporting, billing etc) either via the same browser based customer portal that offers the provisioning, or a separate one, depending on the vendor's approach.

4.21 Use Case 21: Mobile Customers' Identity Authentication Using a Cloud Provider

4.21.1 Description / User Story

Mobile banking has emerged as a significant financial services channel. Mobile banking and other financial services enable customers to pay bills on the fly, check and transfer balances and even trade stocks. Mobile banking usage is set to double the next three years, reaching 400 million people by 2013, according to Juniper Research.

The proliferation of new payments products - such as mobile applications, especially at the front end of the transactions, where initial access is gained - generates ongoing concern around data security, identify theft, fraud and other risk-related issues among consumers, businesses, regulators and payments professionals.

To address issue of the front end of the transaction risk, Identity and Access Management (IAM) technologies for managing the user access control and authentication including Cloud-based identity management solutions offered by Cloud service providers, are leveraged to mitigate this risk.

Cloud-based Identity and Access Management services offered from the cloud such as identity proofing, credential management, strong authentication, single sign-on, provisioning solutions provide organizations with choices and business values such as benefits of cost, reliability, and speed of deployment.

To leverage the aforementioned business values offered by Cloud service provider solutions, a financial company wishes to use Cloud service to authenticate mobile users before routing the financial transaction requested by the mobile users to its back end system hosted at its data centers.

The financial company wishes to leverage the Cloud service provider with numerous data centers located in distributed global locations.

4.21.2 Goal or Desired Outcome

The financial company is able to use cloud service for its global-based mobile clients to make connection to the closest physical location to enhance fast response.

4.21.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ General Authentication • Secondary ○ Federated Identity Mgmt. (FIM) ○ Single Sign-On (SSO)	**Featured Deployment and Service Models:** • Cloud Deployment Models ○ Public ○ Private • Service Models ○ Software-as-a-Service (SaaS)
Actors: • Mobile Client (Customer) • Enterprise administrators • Service provider administrators	**Systems:** • None
Notable Services: • Financial / Banking Services • Cloud Authentication Service • Cloud Management Platform: ○ Single Sign-On (SSO) – User Authentication to Cloud provides credentials needed to Manage/Access Cloud IaaS Services. ○ Multi-factor authentication ○ Access Control Services – Manage Roles and Security Policies (e.g. customer's identification information)	
Dependencies: • Endpoint security for user authentication. • Endpoint transaction security from mobile services. • Compliance to end-to-end security local regulations. • Forensic investigation traceability, capability and availability • On-going verification, certification of the service provider • Service providers' downstream contractors • Trust anchor	
Assumptions: • Company has established an account with the cloud service provider along with any "root" trust credentials to further administer more granular (service or resource level) security policies. • Access Control: Company is able to manage its security policies and associate them to cloud enabled processes ○ The ability to correlate cloud (storage) transactions across infrastructure boundaries	

(i.e. identities and authentications are preserved).

Geography: Consideration of local rules and regulations on personal identifiable information. Authorization would need consider context space (geo-location) of requests.

- Data: Consideration of local rules and regulations on personal identifiable information.
- Storage: Consideration of local rules and regulations on Personal Identifiable Information (PII).

4.21.4 Process Flow

1. A Mobile client logs on to the Financial Institution's (FI) on-line service web-site via mobile device browser.
2. Based on pre-arrangement, the Mobile client is directed to the Cloud authentication hosting site.
3. The Mobile client enters credential for authentication.
4. Mutual authentication is invoked and secure channel is established to secure authentication information and attributes passed over wireless network.
5. Cloud authentication service provider validates the Mobile client credential (user credential and device credential (mobile phone number, other mobile phone attributes.
6. The Mobile client is authenticated and passed forward to the banking system to allow access to the system to conduct financial transaction.
7. Secure connection maintains throughout the session.
8. The Mobile client completes transaction and logs off.
9. Secure channel terminates.

4.22 Use Case 22: Privileged User Access using Two-Factor Authentication

4.22.1 Description / User Story

This use case is concerned with privileged users such as enterprise administrators accessing the management consoles to configure and manage their instance. The administrator can use this console to manage the users, assign privileges or change the configuration for their tenant of the cloud service, whether its IaaS, PaaS or SaaS.

This is a security sensitive operation and it is preferable to require that the administrator to login with Two-Factor Authentication (2FA) such as a PKI certificate or a username/password and an OTP.

An optional element of this use case is that the 2nd factor credential issuance and validation services may themselves be offered as a cloud-based or SaaS offering.

4.22.2 Goal or Desired Outcome

The enterprise can securely manage their use of the cloud provider's service. Further they can also meet their compliance requirements.

4.22.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ Infrastructure Identity Establishment ○ Multi-factor Authentication • Secondary ○ Account and Attribute Mgmt.	**Featured Deployment and Service Models:** • Cloud Deployment Models ○ None featured • Service Models ○ None featured
Actors: • Enterprise Administrators	**Systems:** • Cloud Providers (SaaS, PaaS, IaaS)None
Notable Services: • Cloud Provider Management Console • OTP Server/Service • PKI Certificate Enrollment & Validation Service.	
Dependencies: • Compliance & Audit requirements to track privileged user actions in the cloud.	
Assumptions: • Enterprise administrators have been provisioned with the correct 2FA credentials • The SaaS provider supports the use of 2FA credentials during access. • 2FA (and multi-factor) authentication implies these are privileged users who are generally of interest for compliance and audit standards.	

4.22.4 Process Flow

Option1:

1. The enterprise administrator accesses the URL for management console for the cloud service.
2. The user is prompted to enter 2FA credentials in addition to username and password.
3. Upon successful validation of credentials, the user can access the management console service, and can perform privileged operations.

Option 2:

1. The enterprise administrator accesses the URL for management console for the cloud service.
2. The administrator is redirected to an Identity Provider (IdP) hosted by the enterprise using SAML or any such federation protocol.
3. The enterprise IdP prompts them to enter 2FA credentials in addition to username and password.
4. Upon successful validation of credentials, the user is redirected back to the cloud provider with the appropriate assertion and can access the management console service, and can perform privileged operations.

4.23 Use Case 23: Cloud Application Identification using Extended Validation Certificates

4.23.1 Description / User Story

This use case is about identifying the cloud/SaaS application to the user. The SaaS application has been configured to use Extended Validation (EV) certificates. When the user accesses the SaaS application, the web-browser turns an element of the address bar green to indicate that the user is going to a trusted site.

4.23.2 Goal or Desired Outcome

The end-user is assured that they are connecting to a valid trusted site that belongs to the SaaS application, and that any information that they provide to the website will be secured using SSL encryption.

4.23.3 Notable Categorizations and Aspects

Categories Covered: ***Select one or more from:*** • Primary ○ Infrastructure Identity Establishment • Secondary ○ None	**Featured Deployment and Service Models:** • Cloud Deployment Models ○ None featured • Service Models ○ Software-as-a-Service (SaaS)
Actors: • Subscriber End-user	**Systems:** • Cloud Provider Identity Mgmt. System, that supports: ○ Client Browsers with EV Certs. ○ SaaS Applications
Notable Services: • SaaS applications • Cloud Provider EV Certificate Services	
Dependencies: • Support for standardized EV Certificates	
Assumptions: • User is using a version of browser that supports the security trust indicator for EV certificates • The SaaS application is using SSL with an EV certificate.	

4.23.4 Process Flow

1. A Subscriber End User visits the cloud hosted SaaS application.
2. The SaaS application uses an EV certificate; this enables the security trust indicators in the user's browser.
3. The user is assured about the trust-worthiness of the cloud provider and can continue accessing the application.

4.24 Use Case 24: Cloud Platform Audit and Asset Management using Hardware-based Identities

4.24.1 Description / User Story

One of the interesting aspects of the paradigm-shift to cloud-based computing is that of the need of Enterprises utilizing cloud computing services to maintain the same degree of audit and logging services/capabilities as found in the conventional scenario where all IT functions occurred within the physical boundaries of the Enterprise. Such audit and logging capabilities are needed for the Enterprise to fulfill regulatory compliance requirements (e.g. SOX, HIPAA, HIT), but also for resolving disputes in the case where attacks, breaches and other disaster-related events occurred in the cloud infrastructure that affects the Enterprise customers.

Enterprises today are very much concerned about access control, configuration management, change management, auditing and logging. These issues represent an obstacle to Enterprises fully embracing cloud computing. Most Enterprises today only operate non-core applications in cloud, while retaining dedicated hardware internally to operate business-critical and sensitive applications. The fact that today many cloud-based service providers (e.g. SaaS, PaaS, etc) operate multi-tenant cloud infrastructures adds the complexity of proving trustworthiness of the cloud-based computing environment.

For the cloud provider, the server pool model based on virtualization technologies allow virtual server stacks to be “moved” from one server hardware to another. Though this approach provides efficiency through resource sharing, there remains the issue of proving non-interference in the multi-tenant scenarios and establishing ``proof of execution'' (of a given application) for the Enterprise customer.

The notion of ``proof of execution'' is core to the ability of an Enterprise to provide evidence that an employee operated an application software (albeit at a remote cloud provider) and accessed certain resources. This is particularly relevant in circumstances where the Enterprise is seeking to provide evidence to a third-party auditor entity. Core to this proof of execution is a persistent hardware-based identity is visible to the hypervisor layer and to the operating systems functioning above, and is the basis for tracking and logging. This identity must be traceable and logged as part of the audit trail for the Enterprise customer

4.24.2 Goal or Desired Outcome

A desired outcome would be one or more profiles or specifications that build on existing standards for hardware-based identity (e.g. TCG TPM1.2 specs) and exposing these hardware-identities to the relevant software tools.

4.24.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ Infrastructure Identity Establishment ○ Audit and Compliance • Secondary ○ None	**Featured Deployment and Service Models:** • Cloud Deployment Models ○ Private ○ Public • Service Models ○ Infrastructure-as-a-Service (IaaS)
Actors: • Enterprise • Cloud Provider • Employee • Auditor	**Systems:** • Cloud Management Platform • Cloud Asset Management Systems and Configuration Mgmt. Databases (CMDB)
Notable Services: • Logging • Asset Tracking • SSO • Endpoint Authentication	
Dependencies: • Cloud provides utilize virtual platforms (and virtual machines) that support the notion of "proof of execution" and hardware identities that can be tracked for the purposes of audit and compliance against various government and industry compliance frameworks.	
Assumptions: • None listed	

4.24.3.1 Categories Covered

- ***Establishing Trust in Cloud Infrastructure***: In order for Enterprise customers to develop technical trust and social trust in the infrastructure of a cloud provider, there needs to be a hardware-based identity that is the root-of-trust for all software executing on that piece of hardware. This hardware-based identity must satisfy a number of security requirements, and must be a key part of the asset management mechanisms used by the cloud provider. The hardware-based identity must also be the basis for proving (disproving) multi-tenancy following the request of a customer.

- ***Audit***: Every Enterprise today needs to follow compliance regulations. Currently Enterprise have full control over their IT infrastructure because these are operated internally by the Enterprise. Since internally the various IT functions are allocated across fixed servers, tracking and auditing tasks can be done using current asset management, ITIL and CMDB based tools. Even in the case of virtual servers inside that IT infrastructure, the IT personnel knows which physical servers have been allocated for running virtual servers. The case is somewhat more obscure when an Enterprise uses an external cloud service provider (e.g. PaaS). The Enterprise has no insight into which physical machine its Application is running on. Furthermore, the Enterprise (and Third Party Auditors) have no way to verify that its Application is running either in a multi-tenant infrastructure or dedicated pools of hardware.

4.24.3.2 Applicable Deployment and Service Models

- ***Cloud Deployment Models:***
  - *Private*: Hardware-based identities that can be traced and logged provide Enterprise (running private clouds) with more control over the execution environment of its applications. It provides a "handle" for asset management tools to track devices.
  - *Public*: In public cloud computing environment, the Cloud Provider needs to make persistent hardware-identities visible and traceable to its Enterprise customers.
- ***Service Models***:
  - *Infrastructure-as-a-Service* (IaaS): In the IaaS scenarios, persistent hardware-identities should be accessible to the tracking and audit tools that the Enterprise may choose to also deploy on the platform. In this case the task of collecting the traces and creating the logs belongs to the Enterprise. The IaaS Provider may need to provide some APIs to the underlying infrastructure components that is allocated to the Enterprise customer.
  - *Platform-as-a-service (PaaS):* In the PaaS scenario the Enterprise is typically further removed from the hardware layer, and thus from the hardware-bound identities. The PaaS provider must therefore manage both the hardware-layers and the virtualization layers, and provide some APIs to the Enterprise applications to allow the Enterprise to obtain a log of the bindings between the hardware-layer and virtualization-layers for audit purposes.

4.24.3.3 Actors

- *Enterprise*: This is the legal entity that buys services from the Cloud Provider (eg. PaaS, IaaS).
- *Cloud Provider*: This is the entity that offers cloud computing services to the Enterprise. The term "Cloud provider" is used generically to cover providers of various kinds, but all

with a common aspect of operating virtualization layers above a collection of hardware, as a means to gain efficiency in computing performance.

4.24.3.4 Systems

- Cloud Management Platforms:
  - Logging of all users authentications and SSO management.
  - Logging of all software and hardware used to fulfill user's task.
  - Logging of all resources (e.g. files, storage) used to fulfill user's task.
- Cloud Asset Management Systems and CMDBs:
  - Asset-tracking and configuration management using hardware-based identities.

4.24.3.5 Dependencies

- End-point authentication and authorization of users: audit system depends on the user correctly authenticated and access control policies enforced.
- Asset management System and CMDB operates unhindered.

4.24.3.6 Assumptions

- Servers are assumed to have tamper-resistant hardware where identities are maintained. Furthermore, such hardware-bound identities are assumed to be readable/verifiable by the firmware or operating systems in the same physical server.

4.24.4 Process Flow

4.24.4.1 Scenario 1: Enterprise logs the running of an Application (Private Cloud)

1. Employee of an Enterprise runs an Application in the cloud.
2. The running of the Application triggers a process that reads the hardware-bound identity and the writes the identity to an external log.
3. The audit-log infrastructure in the Enterprise periodically collects the servers-logs and VM-logs, and places these logs-data in a separate physical server.
4. When the virtualization infrastructure moves the Application to a different virtualized server (from the server pool), this triggers the process that re-reads hardware-bound identity and the writes the identity to an external log.

4.24.4.2 Scenario 2: Enterprise logs the running of an Application at a Cloud Provider

1. Employee of an Enterprise runs an Application at the Cloud Provider.
2. The running of the Application triggers a process that reads the hardware-bound identity and the writes the identity to an external log maintained by the Cloud Provider.
3. The audit-log infrastructure at the Cloud Provider periodically collects the servers-logs and VM-logs, and places these logs-data in a separate physical server. These logs are structured and periodically signed by the Cloud Provider

4. When the virtualization infrastructure at the Cloud Provider moves the Application to a different virtualized server (from the server pool), this triggers the process that re-reads hardware-bound identity and the writes the identity to an external log.
5. The Enterprise customer periodically downloads the signed logs from the Cloud Provider, and maintains them for future audit and compliance requirements.

4.25 Use Case 25: Inter-cloud Document Exchange and Collaboration

4.25.1 Description / User Story

Interoperability is of historically observable importance (e.g. email). In defining Inter-cloud interoperability models, issues of identity are central and unavoidable.

In particular, businesses trading with one another want to be able to collaborate and exchange business documents between their respective systems, which are increasingly cloud-based. Such exchanges are already possible in many cases today, but typically require relatively high-cost and non-standardized setup processes.

Two convergent use cases arise:

1) **"Three-corner"**: a term used for the most common, current model whereby both parties must have an identity on the same system. This becomes problematic for suppliers in particular, who may need to establish identities on many different clouds to connect with their various customers. Integration models exist; however, these only apply once an identity and routing have been established. No standard model or profile has been established for the use of existing identity standards in this context.
2) **"Four-corner":** a model explicitly defined as an exchange between two clouds (i.e. service providers) or systems, each acting as a proxy for one party to a business relationship. Regarding identity and trust, however, no model beyond peer-to-peer trust arrangements and document signature has been defined.

4.25.2 Goal or Desired Outcome

Business entities trading with one another should be able to seamlessly establish new electronic trading relationships via their existing cloud business and commerce systems. In particular, it should be possible to set up the identities and relationships required on the various cloud systems with zero or minimal user intervention.

4.25.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ Federated Identity Mgmt. (FIM) ○ General Authentication • Secondary ○ Authorization ○ Account and Attribute Management ○ Account and Attribute Provisioning	**Featured Deployment and Service Models:** • Cloud Deployment Models ○ Hybrid • Service Models ○ Integration-as-a-Service (see service model definition below)
Actors: • Receiver Company • Receiver Administrator • Sender Company • Sender User • Sender Administrator	**Systems:** • Commerce Cloud Services • Identity Store • Intercloud Root
Notable Services: • Delivery Channel Service • Identity Attribute Query/Create/Update Service • Collaboration Authorization Service	
Dependencies: • Identity Attribute (Collaboration Profile) Specification • Collaboration Protocol Agreement Negotiation • Trust Framework Scaling, but perhaps not initial deployments, may depend on the following: • Federated Identity Store Discovery Service (Inter-cloud Root) • Federated Identity Store Peering Model	
Assumptions: • A Trust Model exists enabling certain levels of upfront trust between Commerce Clouds, without human intervention	

4.25.3.1 Featured Deployment and Service Models

- ***Cloud Deployment Models:***
  - *Hybrid:* by definition, this scenario involves at least two clouds (one for each party), and probably more, with different cloud systems handling different layers, and performing different roles in enabling an end-to-end connection.
- ***Service Models***:
  Integration-as-a-Service

The function of “Cloud Brokerage”, i.e. intermediating between different Cloud APIs, is also sometimes referred to as “integration-as-a-service”. This has not yet generally featured in standard taxonomies of cloud service models.

This use case features **Integration-as-a-Service**, but serves to connect clouds that provide the following service models:

- **Software-as-a-Service (SaaS)** - the Cloud business systems to be connected are software application systems
- **Platform-as-a-service (PaaS)** - some of the Cloud systems to be connected in this use case context exist as a PaaS, but as platforms that are tightly bound to an API for a specific SaaS system, rather than as generic application platform environments.

4.25.3.2 Actors

- *Receiver Company*: organization or person receiving a business document via a specified channel
- *Receiver Administrator*: if the Receiver Company requires human approval of new trading partner setup requests, the user who is authorized to approve such requests.
- *Sender Company*: organization or person sending a business document to a trading partner.
- *Sender User*: the user at the Sender company whose email address is the basis for identity matching within the Receiver’s system, based on the use of that email address in documents each party emails to the other.
- *Sender Administrator*: if Sender Company has a pre-existing account on the Receiver Commerce Cloud, the person who controls access to that account.

4.25.3.3 Systems

- *Sender Commerce Cloud*: cloud service that sends all of a Sender Company’s commerce transactions of a particular type to recipients (a) via certain sender-designated channels (e.g. email), but also (b) via receiver-designated electronic channels for Receiver Entities discovered to be compatible through querying an Identity / Identity Attribute Store.
- *Receiver Commerce Cloud*: cloud service that receives and electronically processes transactions of a particular type on behalf of a Receiver Company.
- *Identity Store*: a store with a service interface allowing the retrieval of information about entities and their attributes, including collaboration services they support. Attribute information is retrieved through pointers to corresponding Identity Attribute Stores. An Identity Store is a component of a Commerce Cloud.
  - An *External Identity Store* contains identity information from external sources, i.e. other, federated Identity Stores.
  - An *Internal Identity Store* for a company contains identities from processes internal to that company. Internal identities may or may not have been matched with external identities.
- *Identity Attribute Store:* contains Attribute records about certain services supported by a Company. Identity Attributes in a Store may be managed either (a) by that Identity Attribute Store Provider, or (b) by the Company itself, via its own designated Identity

Attribute Store. Records may be stored in one addressable source Identity Attribute Store, or may be cached, replicated or synchronized to other Identity Attribute Store.

- *Inter-cloud Root Identity Store*: a single root system with which certain compatible Identity Stores are synchronized, directly or indirectly.

4.25.3.4 Notable Services

- *Delivery Channel Service*: originates or receives a specified type of Document Exchange, coupled with a specified Transport or Service endpoint.
- *Identity Attribute Services*: queries, creates or updates an Attribute record for a particular service supported by an Identity in an Identity Attribute Store.
- *Collaboration Authorization Service*: enables the authorization and fulfillment of a request by a trading partner to collaborate electronically, by matching identity attributes corresponding to that partner between the submitted request and internal systems. If authorized, the service also negotiates and configures the electronic collaboration between the parties.

4.25.4 Process Flow

In general and overall, the full use case includes the following steps or scenarios:

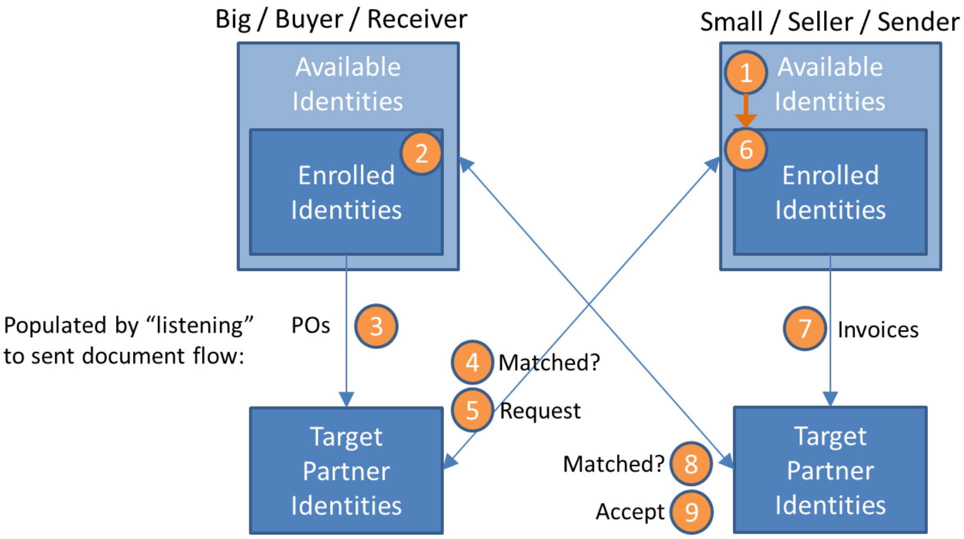
I. Establishing trust between Commerce Clouds via some Inter-cloud Trust Framework;

II. One party, (Receiver), enrolling with, and delegating authority to a Commerce Cloud to initiate and manage collaboration with its partners;

III. The matching by each party of External and Internal Identities for the other;

IV. Delegation of authority by Sender for the Commerce Clouds to act on their behalf;

V. Mutual authorization of Sender-Receiver collaboration via the Commerce Clouds;



4.25.4.1 Scenario 1: Partner Identity Matching and Authorization

1. A Sender Company has a relationship with a Sender Commerce Cloud, and has authorized it to create a publicly-searchable identity on the Sender Commerce Cloud and, through it, other federated Commerce Clouds (such as the Receiver's). The Sender Company need not have enrolled upfront with the Sender Commerce Cloud for activation of certain available Collaboration Services (that is, Sender may or may not have authorized Sender Commerce Cloud to act on its behalf in authorizing third party access to such services).
2. A Receiver Company wants to receive certain documents (e.g. invoices) electronically from its various business partners, including Sender. Receiver has enrolled with Receiver Commerce Cloud, this is, has authorized it to meet this goal by implementing certain electronic business collaboration processes with those partners.
3. The Receiver Commerce Cloud is connected to Receiver's process for emailing certain documents to its business partners (e.g. purchase orders). Through this process, the Receiver Commerce Cloud populates its Internal Identity Store with identities for

partners (including Sender) based on those email addresses. Internal Identities are pre-authorized for access to the Receiver Commerce Cloud services required for collaboration with Receiver.

4. The Receiver Commerce Cloud looks up the Sender Company in the Receiver Commerce Cloud's External Identity Store (based on an email address, for example) and, if matched, retrieves from the indicated Identity Attribute Store a Sender Profile Record that specifies:
    a. Sender Identity Attributes, including Trust Level/Certificate information;
    b. Sender Collaboration Profile, specifying available Delivery Channels, each with their Availability/Activation status;
    c. Sender Collaboration Authorization Service, specifying a Delivery Channel and any validation/trust requirements.
5. Receiver Commerce Cloud calls the Sender Collaboration Authorization Service, with a proposed Collaboration Agreement including:
    a. Process Specification, defining the business interactions (e.g. e-invoicing);
    b. Delivery Channels to be activated for Sender and Receiver respectively;
    c. Receiver Identity Attributes, including Trust Level/Certificate information;
    d. Collaboration Attributes (e.g. account and/or transaction information, Sender's account number with Receiver and/or vice versa; Purchase Order or other transaction reference number);
    e. Security Token for Sender (or their Commerce Cloud) to connect with Receiver via the specified Delivery Channels (e.g. an OAuth token for a pre-authorized Sender Account on the Receiver Commerce Cloud).
6. Sender enrolls with Sender Commerce Cloud, that is, authorizes it to activate the proposed collaboration with Receiver. Directly or through delegation, Sender also so authorizes Receiver Commerce Cloud (See Scenario 2, User Authority Delegation for Collaboration).
7. The Sender Commerce Cloud, once authorized, is connected to Sender's process for emailing certain documents to its business partners (e.g. invoices). Through this process, Sender Commerce Cloud populates its Internal Identity Store with identities for partners (including Receiver) based on those email addresses. Such Internal Identities are pre-authorized for collaboration with Sender by accessing the relevant Sender Commerce Cloud services.
8. Sender Commerce Cloud can then, once authorized, automatically and synchronously, attempts to match the Receiver Identity Attributes presented (including any certificates) with a pre-authorized Internal Identity.
9. Sender Commerce Cloud responds (but possibly asynchronously, and with multiple status update messages, in the event additional Sender Administrator authorization is required), including:
    a. Confirmed Collaboration Agreement Process Specification, defining interactions between the parties;
    b. Security Token for Receiver (or their Commerce Cloud) to connect with Sender for the specified interactions.

10. Receiver Commerce Cloud may send a further response to Sender Commerce Cloud, if needed with:
    a. Security Token(s) authorizing Sender Commerce Cloud to Access to the Agreed Receiver Services Profile (e.g. if the initially sent token was for Request only, with Access authorization being granted only after receipt of the Confirmed Collaboration Agreement);
    b. Confirmation of Receiver Services setup, per the Collaboration Agreement.

4.25.4.1.1 Scenario Dependencies

1. Inter-cloud Trust Framework, i.e. for trust between Commerce Clouds (see Scenario 3)
2. Identity Store. Can be either a:
    a. Centralized Identity Store, shared by all interconnected Commerce Clouds, or a
    b. Federated Identity Store, with Identities replicated via either a
        i. Peering Model, or a
        ii. Hierarchical Model, i.e. an Inter-cloud Root,

4.25.4.1.2 Scenario Assumptions

1. Receiver has previously enrolled with, i.e. authorized Receiver Commerce Cloud to act on their behalf (see Commerce Cloud Authority Delegation).
2. External/Internal Sender identity match is based on a single email address rather than, say, different email addresses on the same domain (which raises additional authorization issues).

4.25.4.2 Scenario 2: User Authority Delegation for Collaboration

Sender User enrolls with Sender Commerce Cloud, that is, authorizes it to activate the proposed collaboration with Receiver. Directly or through delegation, Sender User also so authorizes Receiver Commerce Cloud. Sender's authorization process here includes:

1. Sender User authorizing the Sender Commerce Cloud:
    a. With this Receiver, to activate collaboration via Receiver Commerce Cloud;
    b. Optionally, with other future partner requests, to automatically activate (based on a specified trust validation process);
    c. Optionally, with other future partner requests, to assert this delegated authority (1(b)) to such a partner's Commerce Cloud which, if trusted, substitutes for them obtaining direct Sender authorization.
2. Sender User authorizing the Receiver Commerce Cloud to activate Sender Commerce Cloud access as Sender's proxy, either:
    a. Directly and explicitly, by Receiver Commerce Cloud emailing Sender User a link to grant authorization (if Sender Commerce Cloud is not trusted to do so);

   b. Indirectly and explicitly, by trusting Sender Commerce Cloud to email Sender User a link to grant the required authorizations (if not previously authorized by Sender);
   c. Indirectly and implicitly, by trusting Sender Commerce Cloud's assertion of delegated authority (if previously so authorized by Sender).

4.25.4.2.1 Scenario Assumptions

1. External/Internal identity match is based on a single Sender User email address rather than, say, different email addresses on one domain (which raises additional authorization issues).

4.25.4.3 Scenario 3: Inter-cloud Trust Establishment

1. The Receiver Commerce Cloud establishes trust in the Sender Commerce Cloud's assertions of Sender-delegated authority through a Trust Model, i.e. either:
   a. A Trusted Agreement between the two Commerce Clouds; or
   b. A Trust Framework, establishing a chain of trust between the Commerce Clouds indirectly, via one of more trust intermediaries; or
   c. A Trust Lookup, that is, of an Identity Attribute for the Sender Company from a public record they are known to control (e.g. their DNS domain record). This would authenticate the Sender Commerce Cloud as a proxy for Sender (e.g. as the endpoint for the Sender Collaboration Authorization Service).
2. Such a Trust Framework or Agreement enables some level of upfront trust between Commerce Clouds acting as proxies or delegates for their respective users, i.e. without a direct and explicit human authorization step (see Scenario 2, User Authority Delegation). Specifically, a Trusted Commerce Cloud publishing a user identity with associated attributes, such as email or domain:
   a. MUST obtain that user's agreement before publishing such an Identity, and any Attributes/Services associated with it;
   b. MUST, for each such user Identity Attribute:
      i. declare a Trust Level as defined in the Trust Framework Agreements; and
      ii. obtain verification or certification by a process conforming with the requirements defined for such a Trust Level (e.g. for "Basic" trust in an email address, by the user clicking a link in a verification email)

1. MUST act on behalf of that user in accordance with agreed Terms of Service and Privacy Policy, where such Terms of Service and Privacy Policy also conform to any requirements in the Trust Framework Agreements.

4.25.4.3.1 Scenario Assumptions

1. No previous relationship exists between the Commerce Clouds for Sender and Receiver. This is the first document to be delivered from and any user of one cloud to any user of the other.

4.25.4.4 Scenario 4: Identity and Attribute Management

1. A Sender Company, via its Commerce Cloud, wants to be able, in turn, to receive documents, and potentially payments, from Receiver Entity, via its Commerce Cloud.
2. The Sender, via its Commerce Cloud, wants to ensure that the Sender Identity Attributes for addressing/routing that are stored in the Receiver Commerce Cloud Identity Attribute Store are securely added or updated as required.
3. The Sender Commerce Cloud Identity Store triggers transmission to the Receiver Commerce Cloud Identity Attribute Store of any new or updated Sender Identity Attributes by one of the following mechanisms:
    a. Directly Calling the Receiver Commerce Cloud Identity Attribute Store;
    b. Direct Peering: sending the update via a publish-subscribe relationship between the Receiver and Sender Commerce Cloud Identity Stores (and possibly others). This process might be established per identity, or for all records in either Identity Store.
    c. Hierarchical Peering: as above, but with a model involving an Inter-cloud Root.

4.25.4.4.1 Scenario Assumptions

1. The Sender Commerce Cloud is assumed to have been authorized to manage a Sender identity on the Receiver Commerce Cloud Identity Store (see Scenario 2, User Authority Delegation).

4.26 Use Case 26: Identity Impersonation / Delegation

4.26.1 Description / User Story

Customers of the cloud provider may require a cloud provider to supply support that permits one identity to impersonates the identity of another customer without sacrificing security. One instance is when a support representative needs to troubleshoot issues that are only seen by the rights and roles given to the end-user.

4.26.2 Goal or Desired Outcome

Standards exist for to handle the auditing, security, and functionality of impersonating customer identities.

4.26.3 Notable Categorizations and Aspects

Categories Covered:	**Featured Deployment and Service Models:**
• Primary ○ General Identity Mgmt. ○ Authentication • Secondary ○ Account and Attribute Mgmt. ○ Audit and Compliance	• Deployment Models ○ None featured • Service Models ○ None featured

Actors:	**Systems:**
• Cloud Provider support technician • Cloud provider customer	• Cloud Provider Identity Mgmt. System, helps manage resources such as: ○ Cloud customer identity stores ○ Cloud support identity stores
Notable Services: • Cloud Identity Provider Services	
Dependencies: • Standards based configuration template (for provisioning identities)	
Assumptions: • Customer approves in a legal fashion that support may act on-behalf-of their customer identity for support purposes. • There must be a means to track the identity delegation, that is auditability of both the delegated and acting identity need to be preserved.	

4.26.4 Process Flow

1. A cloud provider customer calls the cloud provider support desk with an issue that needs troubleshooting.

2. Cloud provider support determines that troubleshooting requires the technician to act on-behalf-of the customer

3. Cloud provider support technician logs into a support application using their support identity.

4. Cloud provider support locates the customer in the system and activates an impersonation operation

5. Logging & auditing capture cloud provider support actions as they perform actions as the customer identity in the cloud.

4.27 Use Case 27: Federated User Account Provisioning and Management for a Community of Interest (COI)

4.27.1 Background

Organizations that service a community composed of a central office, many branch offices and partners or suppliers will operate over a diverse IT landscape composed from each participating entity's own IT infrastructures. These infrastructures may include combinations of Public and Private Clouds along with traditional enterprise IT environments (hybrid cloud). A standard means to support and federate global identification, authentication and access management services need to be provided in order to attain efficient information sharing and collaboration for such communities.

In this use case, an organization seeks to provide HR Services to a Community of Interest (COI) where identities along with their attributes must be provisioned from a Central Office which operates with multiple Branch Offices in a federated environment of autonomous IT enclaves. These enclaves can provide their own technology and services to their own specific customer base in regional geographies located all over the world. Individual accounts and identities are owner by Branch offices; however, a user's identity must be provisioned and managed to support global access control to information resources in a way so that they can be user across the entire organization.

Additionally, other trusted entities such as suppliers and partners may also contribute identities, all for the purpose of accessing and sharing information resources to provide additional services to the organizations users or customers. Conversely, the subject organization identities must be provisioned in partner systems for sharing their resources. The identities, including their attributes, need to be made available to access control systems in a standard way.

4.27.1.1 Organization Architecture

The organization described in this use case has a complex architecture that provides Human Resource (HR) services directly or through partners. These HR services are offered as part of a cloud-based Software-as-a-Service (SaaS) application on a hybrid or community cloud. Furthermore, these services are be accessed and managed across a complex hybrid IT infrastructure that includes private cloud, public cloud and traditional deployments.

In this system, The Branch Office HR system in this model is responsible and accountable for keeping its users' data up to date in the central HR database Individual users are responsible and accountable for keeping their records up to date in the HR database for a given set of attributes they are allowed to manage such as phone number, email address, IM chat handle and other pertinent personnel information.

Branch Offices serve as the authoritative source for a set of user identities and their attributes they are designated to manage on behalf of the organization. They also may provide identity "tokens" (e.g. software based keys and certificates, mobile devices or chips, physical ID cards, etc.) that can be presented as valid identification at that branch office.

The Provisioning System may work in conjunction (or be integrated) with the HR system to draw required attributes which can be used to establish accounts and identity attributes that are valid for establishing access control and policy management. Specific HR services, identity tokens, identity attributes and access control mechanisms/services may differ from Branch Office to Branch Office depending on local or regional capabilities, requirements and policies.

4.27.2 Goal/Desired Outcome

Provide a means to address the following issues:

- For organizations that have a complex community or hybrid cloud deployment, a means is necessary to provision of users and establish and distribute their identities and identifying attributes among various central and branch offices of an organization.
- The organizations employees, data managers and people from these distributed domains such as suppliers, business partners, and customers are able to use these identities and identifying attributes to authorize access to appropriate information resources, applications and services (perhaps through Software-as-a-Service (SaaS) applications).

4.27.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ Federated Identity Mgmt. ○ Account and Attribute Management ○ Account and Attribute Provisioning • Secondary ○ General Identity Management	**Featured Deployment and Service Models:** • Deployment Models ○ Hybrid • Service Models ○ Software-as-a-Service (SaaS)
Actors: **The following actors appear in the use case's scenarios:** • **COI Users** (Partner, Supplier, Organization) Individuals belonging to a particular part of the organization. They may be employees of a particular Branch Office or Partner and subject to a Branch Office HR system or Partner IT System which owns their primary indentity. • **COI HR Administrators** – Privileged users responsible for entering a user into the HR system of a particular Branch or Central Office within the Organization. • **COI Registrars** – Privileged users that verify identity and credentials of individuals (new users), in preparation of issuing digital credentials valid for their assigned branch. They may enter users' biometrics and other identifying information into the Branch or Central HR System. • **COI Data Manager** (or Data Administrator) – Privileged users responsible for the configuration of access control to data, resources and services provided by the organization's IT systems to COI users.	**Systems:** The following systems are descried in the use case: • **HR System** (Central / Branch Office) - Holds the data on COI Users (Employees, Suppliers, Partners, Administrators among others). • **Identity Provisioning System** (Central / Branch)– Provisions COI Users' accounts in access control systems for services provided by a particular Branch Office. This must also support "Just In Time" (JIT) provisioning of unanticipated (visiting) users. • **Access Management System** (Central / Branch) – COI Users' attributes (privileges) and supports IT functions, either indirectly by supplying attributes to access control systems or possibly directly by providing • **Identity and Attribute Management Systems** – Manages global and local identities, identity attributes for all Organizational users including support on-demand provisioning and synchronization. This includes managing updates to reflect changes in security, access and governance policies.
Notable Services: • Identity Provider Services	

- Access Management / Control Services
- Account, Identity and Attribute Provisioning Services
- Identity and Attribute Synchronization Services

Dependencies:

- Each entity that participates in overall organization (e.g. Branch Office, Partner, etc.) has established a trust relationship through the Central Office and has a means to security identify and message data to each other.

Assumptions:

- The organization operates Software-as-a-Service (SaaS) applications both on premise and off premise in both public and private clouds.
- The organization has agreed upon a standardization for representing a common set of user identity attributes used to govern/control access to the organization's information.
  - Each participating entity in the organization may establish and manage additional attributes for their own local applications and services.
  - Note: Identities are provided by the parent organizations (i.e. Central Office) versus identities being provided by a Trusted Third Party or Cloud Provider.
- Identity and Access Management (IAM) systems support security abstraction by enabling access management without disclosing user information or repositories directly to applications and
- Security Policies have been developed for accessing data and establish accepted levels of assurance for user credentials.
- A minimum set of Global Identity Attributes common to the organization/community has been established. Policies and procedures exist for managing these attributes across the organization.
- Policies and process for release of identity attributes to entities within the organization have been established.
- Service contracts exist for interfacing to the organization's systems(e.g. the global HR System).
- Methods for Service Discovery and establishing secure protocols to interfaces with identity and access management services has been established.
- Establish something like the Health Care XSPA for reliable, auditable methods of confirming personal identity, official Authorization status and role attributes for other COIs.
- A means to exchange and synchronize identity and attribute data has been established across the organization.

Support for existing Identity and Access Management Standards:

- Support Federated Identity Management using trusted Identity Service Providers (ISPs) (such as those described by the Kantara Initiative) and that there is mechanism in place to validate or revoke trust in these ISPs.
- A standardized policy architecture for enforcement of access control. (e.g. OASIS eXtensible Access Control Markup Language (XACML) which accommodates Policy Administration Points (PAP), Policy Decision Points (PDP)s, Policy Enforcement Points (PEP)s)
- A standard means for participating entities to store, organize, manage and synchronize identity data across deployments (e.g. using Lightweight Directory Access Protocol (LDAP) Directories or Active Directory).
- Use of key management and encryption principles/standards to protect identity and data (e.g. Public Key Infrastructure (PKI)).
- Identities can be established using established software standards (e.g. userid/password, OpenID,

OpenCard, X.509 certificates, etc.) or via physical means (e.g. smart cards, mobile devices, etc.).

4.27.4 Process Flow

The overall goal of this use case is to describe the provisioning identities from multiple Branch Offices in a federated environment of autonomous IT enclaves providing their own technology and services all over the world. Additional other organizations, such as suppliers, must also contribute identities, all for the purpose of accessing and sharing information resources.

This use case includes the following scenarios:

- **Scenario 1**: **Provisioning a New User at a Branch Office**: This case shows how a new user is initially entered into an organization and how their identity and attributes flow throughout the organization. A Branch Office establishes a new user into an HR System and collects their personal information. The HR System helps establish the user's common global identity attributes in order to provision them the Central Office. Other local, branch specific identity attributes are also added to the identity at the Branch Office and identity tokens created for the user.
- **Scenario 2**: **Provisioning of User From Business Partner**: This scenario accommodates a user or partner visiting a Branch Office which does not have an identity record established for that person locally. The user is visiting from a Business partner should be able to provision a local identity using the global identity and attributes from the Central Office and from the Partner's IT system.
- **Scenario 3**: **Provisioning of Access Control**: Branch Office access control systems based on attributes are supplied by the Branch Office Provisioning Service as a baseline. The Branch Office Attribute Service has access to the Global Attribute Service for anticipated people where a batch transfer is appropriate as well as unanticipated people where data would be transferred in a case by case "just in time" basis.

4.27.4.1 Scenario 1: Provisioning a New User at a Branch Office

The following figure shows a use case for on-boarding a new user. The user has not previously been entered into the Central HR System. The Branch Office can be a virtual system, that is relying only on the central HR system without any supporting Branch Office HR system or can be using a Branch Office HR system, but the user is under the cognizance of their Branch Office.

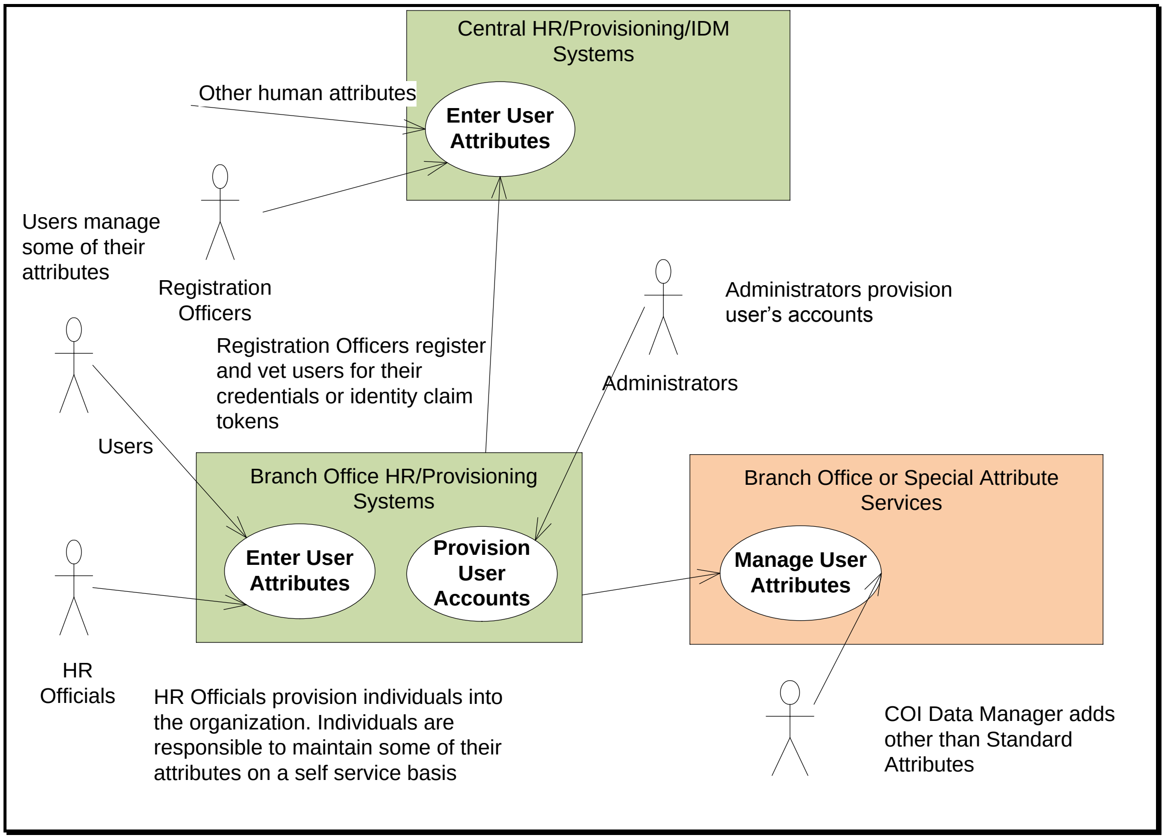

Central HR/Provisioning/IDM Systems
Other human attributes
Enter User Attributes
Users manage some of their attributes
Registration Officers
Administrators provision user's accounts
Registration Officers register and vet users for their credentials or identity claim tokens
Administrators
Users
Branch Office HR/Provisioning Systems
Enter User Attributes
Provision User Accounts
Branch Office or Special Attribute Services
Manage User Attributes
HR Officials
HR Officials provision individuals into the organization. Individuals are responsible to maintain some of their attributes on a self service basis
COI Data Manager adds other than Standard Attributes

FIGURE 5 - PROVISIONING A NEW USER

1. A new Community of Interest or COI User (e.g. a new employee of the organization) provides a standard set of identifying information, credentials and attributes to an COI HR Administrator at the Branch Office who enters it into the Branch Office HR system.
   - 1.1. The common set of identifying information and attributes has been predetermined and agreed upon for use globally by all participating entities in the organization.
   - 1.2. The new user may be responsible for entering some of their own Personally Identifiable Information (PII), such as local phone number or IM address.
2. The Branch Office HR system transmits the new user's information to the Central HR System.

A COI Registrar at the Branch Office collects additional identifying information about the user that has been established to be common to the global organization and additional information that may be specifically required for use at this particular Branch Office.

- 2.1. This may include the user's biometrics if appropriate and other pertinent information in preparation for issuance of some software, hardware or physical identity token (e.g. issuance of a smart card, soft X.509 certificate, or InfoCard, etc.) which can serve as the individual's identity claim at that Branch Office.

   2.2. The Branch Office provisioning system is integrated with the HR system to assist in provisioning the individual into the Branch Office by creating a record with the standard attributes.

3. The Branch Office provisions the identity and its common, global attributes necessary along with any local attributes to the Branch Office IAM systems.

   3.1. This identity provisioning may be coordinated with the Central Office at time of Branch Office provisioning or the Branch Office may be permitted to synchronize at some later time (perhaps against some predetermined schedule).

4. COI Data Managers or Administrators are able assign access control to community services and data using the proper identity attributes that have been established at Branch Office applications (and are not part of the HR system's standard collection of attributes) to the new COI User (based upon their responsibilities within the organization).

   4.1. This could be done directly by adding specific identity attributes to the user account or indirectly with assignment of roles with preset entitlements to the user account.

4.27.4.2 Scenario 2: Provisioning User from Business Partner

This scenario accommodates a COI User or partner visiting a Branch Office which does not have an identity record established for that person locally. The COU User is a valid employee of an official Business Partner of the organization. The local Branch Office should be able to provision a local identity using the global identity and attributes from the Central Office and obtain additional identity claim information (attributes) from the user employing Partner IT System as needed.

Note: bulk transfers of identity and attributes for a collection of users can also be done when required.

The following figure illustrates the case where a user from another Branch Office of an Organization or some other Partner Organization arrives at a service desiring access. If their identity policies and credentials are of the proper assurance for the access control policies in effect, they are able to have access to IT resources.

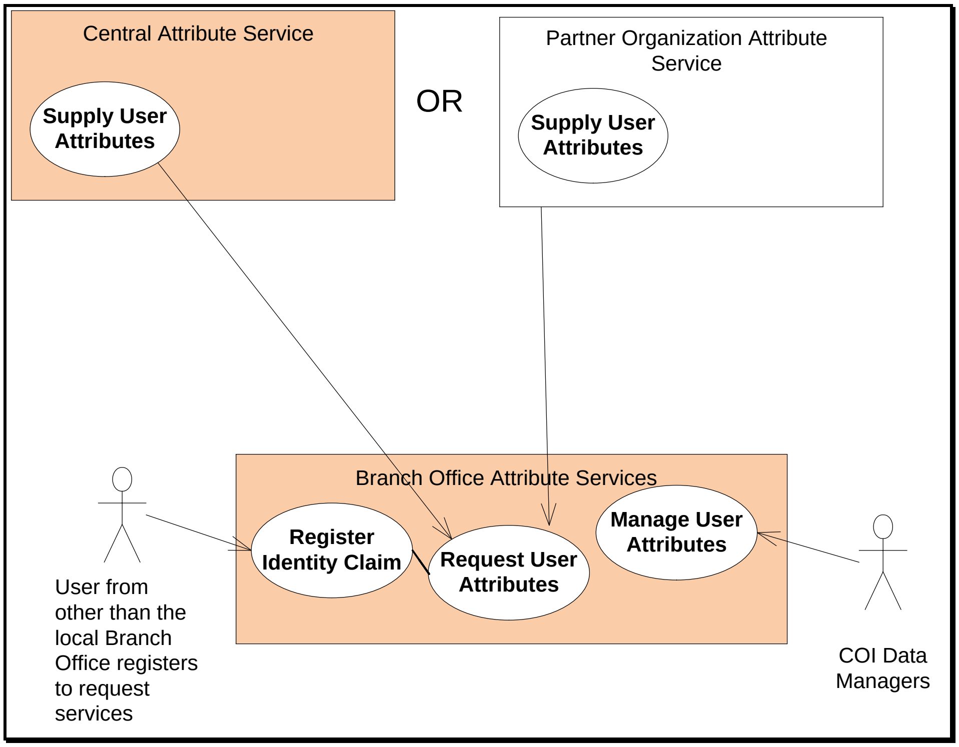

Central Attribute Service
Supply User Attributes
OR
Partner Organization Attribute Service
Supply User Attributes
Branch Office Attribute Services
Register Identity Claim
Request User Attributes
Manage User Attributes
User from other than the local Branch Office registers to request services
COI Data Managers

FIGURE 6 - UNANTICIPATED USER

1. A COI from a Business Partner is visiting a local Branch Office and needs access to organization information or community provided services.

4. A COI Registrar of the Branch Office examines and enters the COI User's identity claims and credentials into their HR and/or IAM system and requests the user's attributes from their Central Attribute Service.

   4.1. If there is no connectivity to the Central Office, by policy a measured amount of default privileges may extended to the user as long as their credentials are within the trust realm of the organization.

5. A COI Data Manager from the Branch Office attaches additional attributes to COI User's newly constructed identity to permit/authorized access to certain systems and data available at that particular Branch Office that this person is entitled to use during their visit.

   5.1. These attributes may be stored locally at the Branch Office

The Branch Office issues the visiting user temporary identity tokens or credentials.

   5.2. These may expire against some policy

4.27.4.3 Scenario 3: Provisioning of Access Control

This scenario demonstrates the importance of having dedicated attribute services as part of access management systems. An Attribute Services may be utilized for supplying a COI Users' attributes directly to applications, services, devices and resources that provide their own access control or indirectly support access control through an abstraction layer characterized by Policy Enforcement Points (PEPs) and Policy Decision Points (PDPs) separate from the applications, services, devices and resources (and made available perhaps from a cloud provider platform).

In this case there are three access control systems for three separate organizations. Additionally, people from all three organizations need to share IT resources from every other organization.

This case shows the organization's COI Data Manager receiving users' attributes from other organizations, either on a planned bulk or "just in time" (JIT) basis and adding any additional attributes necessary for their access control systems for access to the COI controlled data (directly as needed).

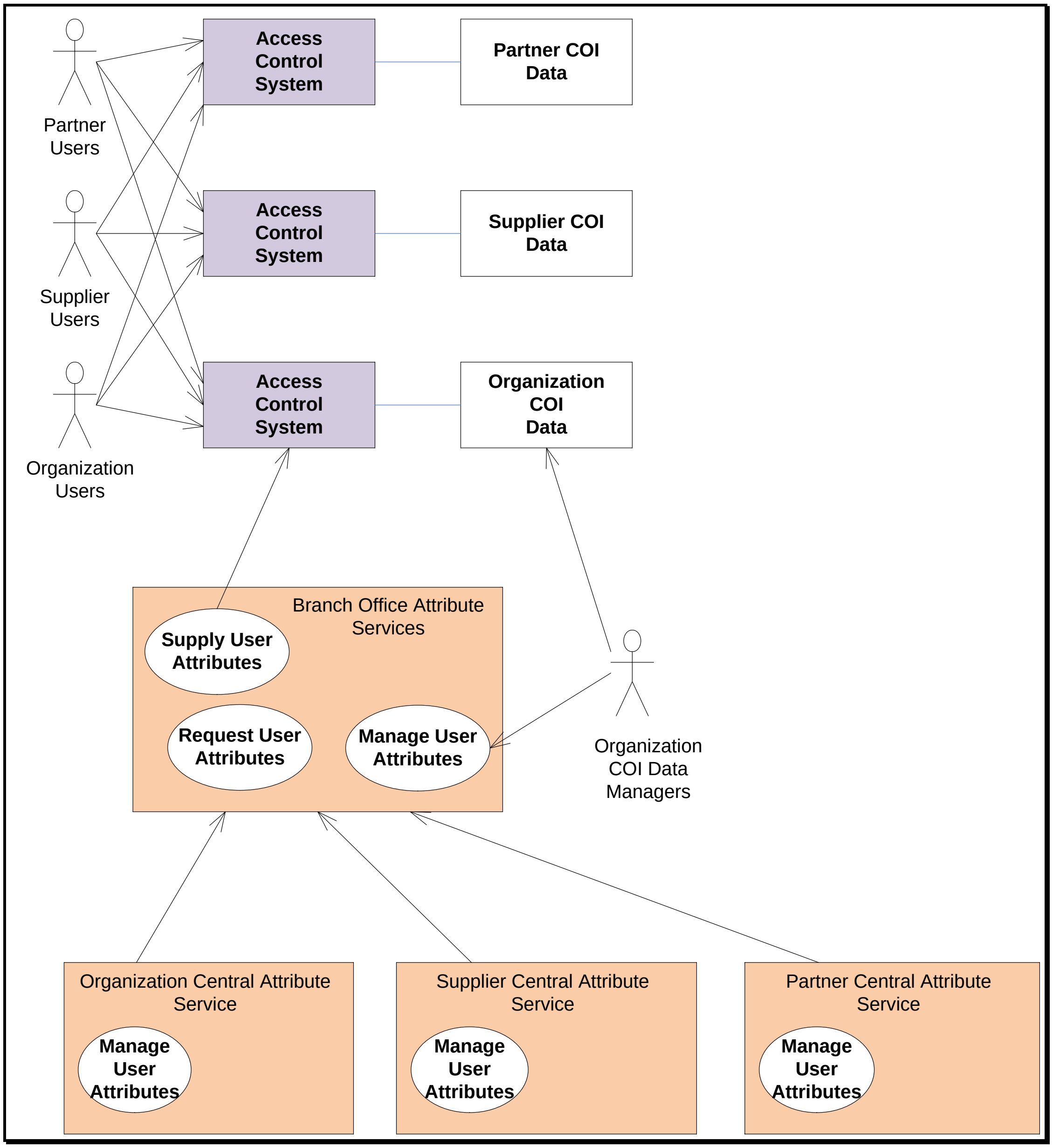


FIGURE 7 - PROVISIONING OF ACCESS CONTROL SYSTEMS

1. The IAM System supporting Branch Offices manage user (identity) attributes provisioned for their respective Branch Office Attribute Services.
2. The Branch Office IAM have dedicated identity attribute services that have the ability to synchronize with the Central Office IAM system and any authorized partner entity approved to provide services to the greater organization.
3. The attribute services have the ability to send and receive required global attributes from the one COI entity (Branch, Partner, etc.) to another as needed (on demand).
4. The COI Data Manager oversees the adding or modifying attributes to the global set of attributes as well as to individual user identity records/entries to enable access control to COI Systems and Data and provides additional local (branch specific) attributes when required.

4.28 Use Case 28: Cloud Governance and Entitlement Management

4.28.1 Description / User Story

In this use case, the service provider (the provider) of a SaaS or PaaS cloud-based application (the application) that contains identity & account authorization, security and entitlement capabilities (the entitlement model) may be obligated to provide information about it's entitlement model so that it may be evaluated, reviewed, and audited by the customer and its agents (e.g. an auditor).

The provider may choose to externalize its entitlement model in a variety of documentation formats (e.g. a structured XML document schema).

Entitlement documentation formats must be machine readable and should enable external management systems to understand and consume its entitlement model for the following purposes

- Creating external enterprise roles that encapsulate application entitlements for the purpose of assignment management.
- Creating entitlement-to-data mapping that facilitates understand what data elements (structured and unstructured) that may be accessed with a given entitlement.

4.28.2 Goal or Desired Outcome

This use case’s goals are to showcase the need for enabling management systems external to cloud deployments that are able to:

- Collect a detailed understanding of what authorization, security and entitlement capabilities are available for assignment to accounts and identities within the application for the purposes of audit and governance.
- Define external encapsulations (roles or managed attributes) that can be used to control account and entitlement provisioning activities.
- Provide security management facilities that detail what resources , services and functions a given authorization or entitlement grants access to (e.g. Entitlement “e1” applies to Service "s1" and grants access to service functions "f1, f2 & f3”).

- Provide security management facilities make cloud entitlement repositories and metadata available as part of an identity governance initiative.

4.28.3 Notable Categorizations and Aspects

<table>
<tr><td><b>Categories Covered:</b>
• Primary
○ Governance
○ Audit and Compliance
• Secondary
○ Provisioning
○ General Account Management</td><td><b>Featured Deployment and Service Models:</b>
• Deployment Models
○ None featured
• Service Models
○ Software-as-a-Service (SaaS) or
○ Platform-as-a-Service (PaaS)</td></tr>
<tr><td><b>Actors:</b>
• Cloud Provider Entitlement Service
• Cloud Based Application (CBA) - <i>This is inclusive of the cloud provider's self service application management functions or services.</i>
• Identity Governance Application (IGA) (external to cloud)
• Account (and User) Provisioning Service</td><td><b>Systems:</b>
• None featured</td></tr>
<tr><td colspan="2"><b>Notable Services:</b>
• <b>Entitlement Service</b> - The cloud provider service (with remote APIs, or service endpoints) that facilitates the request/response protocol for the collection of the defined entitlement model, may be provided by an external application proxy or information provider</td></tr>
<tr><td colspan="2"><b>Dependencies:</b>
• The cloud provider uses a Identity and Access Management System that supports entitlements that can be associated with identities to govern access to cloud based resources.</td></tr>
<tr><td colspan="2"><b>Assumptions:</b>
• It is assumed that the cloud provider hosts an Entitlement Service (with remote API or service endpoints) that facilitates the request/response protocol for the collection of the defined account and entitlement assignments.
• The Cloud Consumer has a means to extend the cloud provider's base entitlements to express those needed for their access control policies, roles and processes at an account and application level.
• The Cloud Consumer has privileged users (or administrators) that are able to invoke the Entitlement Service and Provisioning endpoints or interfaces from their Identity Governance Application (IGA).</td></tr>
</table>

4.28.4 Process Flow

4.28.4.1 Scenario 1: Describe Cloud Provider Entitlement Model

In this scenario, the cloud consumer wishes to examine the cloud provider's entitlement model for their SaaS or PaaS applications.

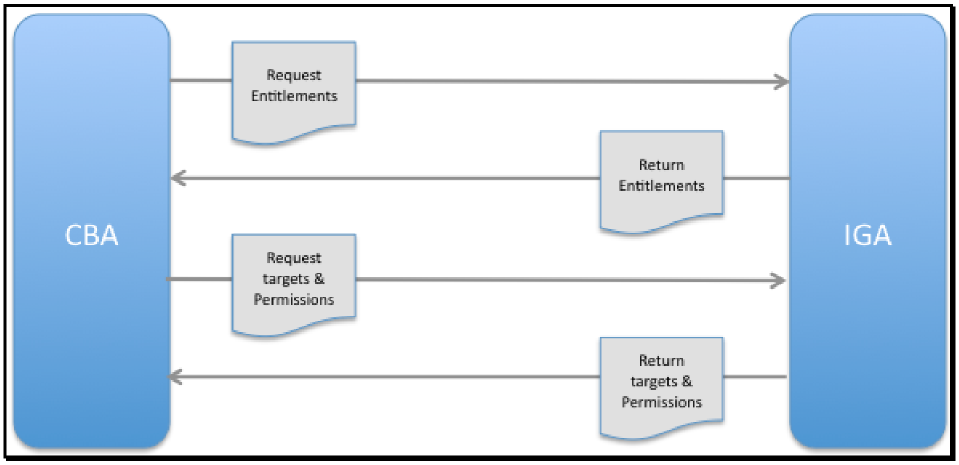


FIGURE 8 - DESCRIBE CLOUD PROVIDER ENTITLEMENT MODEL - PROCESS FLOW OVERVIEW

1. The Cloud Consumer's external Identity Governance Application (IGA) contacts a Cloud Based Application (CBA) (an SaaS or PaaS application) and establishes a secure connection (not shown in figure).
2. The IGA requests a listing of the assignable entitlements model for the CBA either directly from the Cloud Provider's Entitlement Service or indirectly from the CBA itself.
3. The provider's Entitlement Service creates a standards-based document (e.g. a well formed XML document) to export the listing of the assignable entitlement for the referenced CBA and returns it to the calling IGA.
4. The IGA then requests a listing of available target and permissions data available for a specific set of assignable entitlements returned in step 3.
5. The provider's Entitlement Service creates a standards-based (e.g. well formed XML document) to export the available target and permissions data for the specified entitlements and returns it to the calling IGA.
6. The cloud provider is able to produce audit logs that prove policy enforcement using the assignable entitlements for the CBA.

4.28.4.2 Scenario 2: List Account or Application User Entitlements

In this scenario, the cloud provider of a SaaS or PaaS cloud-based applications provides the administrators of their customers accounts the ability to manage (at an account or application level) their users and assigned entitlement capabilities (the entitlement model).

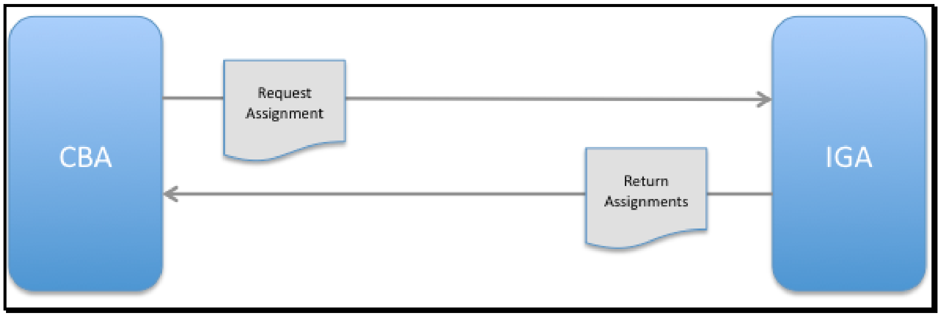


FIGURE 9 - LIST ACCOUNT OR APPLICATION USER ENTITLEMENTS - PROCESS FLOW OVERVIEW

1. The cloud consumer's external Identity Governance Application (IGA) contacts the Cloud Based Application (CBA) and establishes a secure connection (not shown in figure).
2. The IGA requests a listing of the assignable entitlements model for the Users of the CBA either directly from the Cloud Provider's Entitlement Service or indirectly from the CBA itself.
3. The CBA creates a means to export of the hosted application's user accounts and assigned entitlements (application level entitlement model) and returns it to the calling IGA.

4.28.4.3 Scenario 3: Governance Aware Provisioning

This scenario demonstrates the external management of consumer cloud-based applications to create, update and delete accounts and entitlement assignments to those accounts and or its supporting infrastructure.

This scenario is not significantly differentiated from general-purpose (non-cloud based) provisioning capabilities and/or existing standards and protocols. The reason for including it here is to highlight the requirement for value-based, identity enabled services to provide a remote provisioning capability with the consideration for enhanced Identity and Access Governance

Note: In general, this scenario could apply to either use batch or singleton provisioning requests.

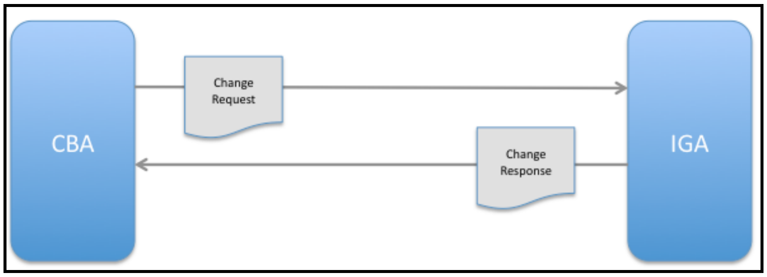


FIGURE 10 - GOVERNANCE AWARE PROVISIONING - PROCESS FLOW OVERVIEW

1. The cloud consumer's external Identity Governance Application (IGA) contacts the cloud provider's Cloud Based Application (CBA) and establishes a secure connection.
2. The IGA requests one of the following change request actions for the cloud-based consumer account (along with any in all required parameters) to the CBA’s provisioning service point:

- Create Account
- Update Account Attributes
- Assign Entitlements
- Remove Entitlements
- Enable/Disable Account
- Delete Account

3. The CBA executes the requested provisioning change and returns status information to the IGA.

4.29 Use Case 29: User Delegation of Access to Personal Data in a Public Cloud

4.29.1 Description / User Story

Alice has subscribed to her own cloud storage provider and has created various files there containing personal data, one of which is her résumé or curriculum vitae (CV) file. Alice wishes to let Bob her friend read her CV file so she needs to delegate read access to him. Bob is not a subscriber to this particular cloud provider, and has no wish to register for yet another set of credentials for accessing yet another service. However Bob does have an account with an Identity Provider that is part of the same federation as the cloud provider, and is trusted by the cloud provider to correctly authenticate Bob.

Alice tells the cloud provider she wishes to delegate read access to a friend for a certain period of time, and the cloud provider returns a secret URL to her, which it has obtained from the delegation service. Alice gives this secret URL to her friend Bob. Bob clicks on the secret URL which connects him to the delegation service, where he is asked to authenticate via his existing IdP. Bob authenticates and the delegation service delegates him access to the CV file (for as long as Alice has determined). Bob can now contact the cloud provider at any time throughout this period. When he does, he is asked to authenticate, which he does via his existing IDP, and he is then granted read access to Alice's CV. Once the delegation has expired he will no longer be granted access.

Use case variants. The secret URL can be one-time use or multiple-use. In the latter case Alice can give the secret URL to a group of people who will each be granted read access to her CV.

Alice can revoke the delegation at any time.

4.29.2 Goal or Desired Outcome

Users are able to use cloud services, such as storage services, and are able to grant access to their friends and colleagues, without the latter having to first register for a user account with the cloud provider. The delegated access can be to a single person or to multiple people, and it can be revoked at any time.

4.29.3 Notable Categorizations and Aspects

Categories Covered: • Primary ○ Governance ○ General Authentication ○ Authorization • Secondary ○ Federated Identity Mgmt. (FIM) ○ Account and Attribute Provisioning	**Featured Deployment and Service Models:** • Cloud Deployment Models ○ Public • Service Models ○ Infrastructure-as-a-Service (IaaS)
Actors: • Consumer User (i.e. Alice) • Delegated Users - that Alice delegates access to for reading her cloud reposited files. • Cloud Service Provider (CSP) • Identity Provider (IdP)	**Systems:** • None
Notable Services: • Cloud Provider Delegation Service (DS) - Manages delegated access to (file) resources. • Cloud Provider IAM Service • Cloud Provider Authorization Service	
Dependencies: • Federated IdM is already in place	
Assumptions: • Federated IdM is already in place to support delegation of access to file resources. • The Cloud Service Provider (CSP) supports a Delegation Service (DS) which manages policies that define file sharing permissions (or entitlements). The description of this policy is out of scope for the current use case. • Use of the OASIS SAML standard to represent security assertions of users. • There is a means to securely share or message file URLs to delegated users which includes encryption (perhaps a service of the CSP security services) of identity tokens and other identity related information. • A Personal ID (PID), in this use case, is an identity token provisioned by the CSP as needed for a delegate user and which should be treated as a shared secret between the CSP and delegate. This function is described here as part of a Domain identity Service (DIS).	

4.29.4 Process Flow

1. Alice, a cloud consumer, logs into her Cloud Service Provider (CSP) where she has a storage account and locates her Curriculum Vitae (CV) file from the file management interface from the CSP's management platform.

2. Alice sets the CV file to "Read Access", selects a time period for the access, and then chooses one or more delegates (other persons or identities known to the provider) she wishes to share her CV file with and clicks “delegate access”.
3. The CSP contacts the Delegation Service (DS) on behalf of the user and asks for an invitation delegation token (a secret URL) for the requested access rights of the user.
4. The DS checks that the delegation is allowed, and if so, returns the secret URL to the user. Otherwise it is rejected.
5. Note: the DS is configured with a delegation policy by the CSP to say which delegations are allowed and which are not. The description of this policy is out of scope for the current use case.
6. The user, Alice, then passes the secret URL to a friend or colleague (a delegate) or multiple people (delegates).
7. Note: The precise mechanism for this is out of scope of the use case.
8. A delegate user clicks on the secret URL, whereupon the DS asks the delegate to authenticate via his preferred IdP.
9. The delegate authenticates to their chosen Identity Provider (IdP) and is then assigned (internally) the delegated attribute by the cloud provider's Domain Identity Service (DIS). The IdP stores the Personal ID (PID) that it uses to refer to the delegate (e.g. a new shared identity token).
10. The delegate goes to the CSP and is asked to authenticate. The delegate chooses the same IdP as before and authenticates successfully to it.
11. The IdP sends the CSP an authentication assertion and a referral attribute that contains the PID of the user encrypted to the DS.
12. The CSP identity decrypts the PID, looks up the delegate's access permissions, and returns a "delegated" attribute (i.e. a permission to access the CV file) to the CSP as a SAML attribute assertion.
13. The CSP can now determine which resource the user has been delegated access to from the contents of the delegated attribute.
14. The delegate is now able to read Alice's CV file.
    14.1. Note: if the delegate attempts the same access steps to read the CV file outside the window Alice permitted for delegated access, the delegate would be denied access and show an appropriate informational error message.

Appendix A. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Chairs

Anil Saldhana, Red Hat

Anthony Nadalin, Microsoft

Editors

Matthew Rutkowski, IBM

Document Contributors:

Abbie Barbir, Individual

Anil Saldhana, Red Hat

Anthony Nadalin, Microsoft

Colin Wallis, New Zealand Government

Dale Moberg, Axway Software

Dale Olds, Novell

Darran Rolls, SailPoint

David Chadwick, Individual Member, University of Kent

Dominique Nguyen, Bank of America

Doron Cohen, SafeNet

Gershon Janssen, Individual Member

Joanne Furtsch, TRUSTe

Kurt Roemer, Citrix Systems

Martin Raepple, SAP AG

Matthew Rutkowski, IBM

Patrick Harding, Ping Identity

Paul Madsen, Ping Identity

Peter Brown, Individual Member

Robert Cope, Homeland Security Consultants

Roger Bass, Traxian

Joe Savak, Rackspace

Siddharth Bajaj, Symantec

Thomas Hardjono, M.I.T. Kerberos Consortium

Tomas Gustavsson, PrimeKey Solutions AB

Technical Committee Member Participants:

Abbie Barbir (Bank of America)

Anil Saldhana (Red Hat)

Brian Marshall (Vanguard Integrity Professionals)

Catherine Tilton (Daon)
Colin Walis (Government of New Zealand)
Dale Moberg (Axway Software)
Dale Olds (Novell)
Daniel Turrisini (Widepoint Corporation)
Darran Rolls (Sailpoint)
Darren Platt (Symplified Inc)
David Chadwick (University of Kent)
David Kern (IBM)
David Turner (Microsoft)
Dominique Nguyen (Bank of America)
Doron Cohen (Safenet)
Gershon Janssen (Individual)
Jeffrey Broberg (CA Technologies)
Jerry Smith (US Department of Defense)
Joe Savak (Rackspace)
John Dilley (Akamai Technologies)
John Tolbert (Boeing Company)
Jonas Hogberg (Ericsson)
Kurt Roemer (Citrix)
Martin Raepple (SAP)
Matt Rutkowski (IBM)
Michael Stiefel (Reliable Software)
Michelle Drgon (Dataprobity)
Patrick Harding (Ping Identity)
Paul Lipton (CA Technologies)
Paul Madsen (Ping Identity)
Peter Brown (Individual)
Robert Cope (Homeland Security Consultants)
Roger Bass (Traxian)
Siddharth Bajaj (Verisign/Symantec)
Stephen Coplan (the 451 Group)
Thomas Hardjono (MIT)
Tom Bishop (Conformity Inc)
Tomas Gustavvson (Primekey Solutions AB)
Tony Nadalin (Microsoft)

Appendix B. Definitions

B.1 Cloud Computing

Cloud computing

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. **[NIST-SP800-145]**

B.1.1 Deployment Models

Private cloud

The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. **[NIST-SP800-145]**

Community cloud

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise. **[NIST-SP800-145]**

Public cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. **[NIST-SP800-145]**

Hybrid cloud

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds). **[NIST-SP800-145]**

B.1.2 Cloud Essential Characteristics

On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service’s provider. **[NIST-SP800-145]**

Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs). **[NIST-SP800-145]**

Resource pooling

The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. **[NIST-SP800-145]**

Rapid elasticity

Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time. **[NIST-SP800-145]**

Measured Service

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service. **[NIST-SP800-145]**

B.1.3 Service Models

Cloud Software as a Service (SaaS)

The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. **[NIST-SP800-145]**

Cloud Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. **[NIST-SP800-145]**

Cloud Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). **[NIST-SP800-145]**

Identity-as-a-Service

Identity-as-a-Service is an approach to digital identity management in which an entity (organization or individual) relies on a (cloud) service provider to make use of a specific functionality that allows the entity to perform an electronic transaction which requires identity data managed by the service provider. In this context, functionality includes but is not limited to registration, identity verification, authentication, attributes and their lifecycle management, federation, risk and activity monitoring, roles and entitlement management, provisioning and reporting. [Source: Wikipedia.]

B.2 Identity Management Definitions

The following terms may be used within this document:

Access

To interact with a system entity in order to manipulate, use, gain knowledge of, and/or obtain a representation of some or all of a system entity's resources. **[SAML-Gloss-2.0]**

Access control

Protection of resources against unauthorized access; a process by which use of resources is regulated according to a security policy and is permitted by only authorized system entities according to that policy. **[SAML-Gloss-2.0]**

Account

Typically a formal business agreement for providing regular dealings and services between a principal and business service provider(s). **[SAML-Gloss-2.0]**

Administrative domain

An environment or context that is defined by some combination of one or more administrative policies, Internet Domain Name registrations, civil legal entities (for example, individuals, corporations, or other formally organized entities), plus a collection of hosts, network devices and the interconnecting networks (and possibly other traits), plus (often various) network services and applications running upon them. An administrative domain may contain or define one or more security domains. An administrative domain may encompass a single site or multiple sites. The traits defining an administrative domain may, and in

many cases will, evolve over time. Administrative domains may interact and enter into agreements for providing and/or consuming services across administrative domain boundaries. **[SAML-Gloss-2.0]**

Administrator

A person who installs or maintains a system (for example, a SAML-based security system) or who uses it to manage system entities, users, and/or content (as opposed to application purposes; see also End User). An administrator is typically affiliated with a particular administrative domain and may be affiliated with more than one administrative domain. **[SAML-Gloss-2.0]**

Agent

An entity that acts on behalf of another entity. **[X.idmdef]**

Anonymity

The quality or state of being anonymous, which is the condition of having a name or identity that is unknown or concealed. **[SAML-Gloss-2.0]** This includes the inability to trace the name or identity by behavior, frequency of service usage or physical location among other things.

Assertion

A piece of data produced by an authority regarding either an act of authentication performed on a subject, attribute information about the subject or authorization data applying to the subject with respect to a specified resource. **[SAML-Gloss-2.0]** An example of an assertion's subject would be an employee and an assertion about them would be that they are a manager (i.e. a named role).

Assurance

See authentication assurance and identity assurance. **[X.idmdef]**

Assurance level

A level of confidence (or belief) in the binding (or association) between an entity and the presented identity information. **[X.idmdef]**

Attribute

A distinct characteristic of an entity or object. An object's attributes are said to describe it. Attributes are often specified in terms of physical traits, such as size, shape, weight, and color, etc., for real-world objects. Entities in cyberspace might have attributes describing size, type of encoding, network address, and so on. Note that Identifiers are essentially "distinguished attributes". See also Identifier. **[RFC 4949]**

Attribute assertion

An assertion that conveys information about attributes of an entity (i.e. an assertion's subject). **[SAML-Gloss-2.0]** An example of an attribute assertion would be that a person with a presented identity (i.e. the entity or subject) has the attributed assertions that they have blue eyes and is a medical doctor.

Authentication

A process used to achieve sufficient confidence in the binding between a person or entity and their presented identity. NOTE: Use of the term authentication in an identity management (IdM) context is taken to mean entity authentication. **[X.idmdef]**

Authentication assertion

An assertion that conveys information about a successful act of authentication that took place for an entity or person (i.e. the subject of an assertion). **[SAML-Gloss-2.0]**

Authentication assurance

The degree of confidence reached in the authentication process, that the communication partner is the entity that it claims to be or is expected to be. NOTE: The confidence is based on the degree of confidence (i.e. assurance level) in the binding between the communicating entity and the identity that is presented. **[X.idmdef]**

Authorization

- The process of determining, by evaluating applicable access control information, whether an enity or person is allowed to have the specified types of access to a particular resource. Usually, authorization is in the context of authentication. Once a person or entity is authenticated, they or it may be authorized to perform different types of access. **[SAML-Gloss-2.0]**
- The granting of rights and, based on these rights, the granting of access. **[X.idmdef]**

Back channel

Back channel refers to direct communications between two system entities without “redirecting” messages through another system entity. **[SAML-Gloss-2.0]** An example would be an HTTP client (e.g. a user agent) communicating directly to a web service. See also *front channel*.

Binding

An explicit established association, bonding, or tie. **[X.idmdef]**

Binding, Protocol binding

Generically, a specification of the mapping of some given protocol's messages, and perhaps message exchange patterns, onto another protocol, in a concrete fashion. **[SAML-Gloss-2.0]**

Biometric (Recognition)

Recognition of individuals based on their consistent behavioural and biological characteristics and measurements.

Certificate

A set of security-relevant data issued by a security authority or a trusted third party, that, together with security information, is used to provide the integrity and data origin authentication services for the data. **[X.idmdef]**

Claim

To state as being the case, without being able to give proof. **[X.idmdef]**

Credentials

A set of data presented as evidence of a claimed identity and/or entitlements. **[X.idmdef]**

Delegation

An action that assigns authority, responsibility, or a function to another entity. **[X.idmdef]**

Digital identity

A digital representation of the information known about a specific individual, group or organization. **[X.idmdef]**

End user

A natural person who makes use of resources for application purposes (as opposed to system management purposes; see Administrator, User). **[SAML-Gloss-2.0]**

Enrollment

The process of inauguration of an entity, or its identity, into a context.

NOTE: Enrollment may include verification of the entity’s identity and establishment of a contextual identity. Also, enrollment is a pre-requisite to registration. In many cases the latter is used to describe both processes **[X.idmdef]**

Entity

Something that has separate and distinct existence and that can be identified in context.

NOTE: An entity can be a physical person, an animal, a juridical person, an organization, an active or passive thing, a device, a software application, a service etc., or a group of these entities. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc. **[X.idmdef]**

Entity authentication

A process to achieve sufficient confidence in the binding between the entity and the presented identity. NOTE: Use of the term authentication in an identity management (IdM) context is taken to mean entity authentication. **[X.idmdef]**

Federated Identity

A principal's identity is said to be federated between a set of Providers when there is an agreement between the providers on a set of identifiers and/or attributes to use to refer to the Principal. **[SAML-Gloss-2.0]**

Federate

To link or bind two or more entities together **[SAML-Gloss-2.0]**

Federation

Establishing a relationship between two or more entities (e.g. an association of users, service providers, and identity service providers). **[SAML-Gloss-2.0] [X.idmdef]**

Front-channel

Front channel refers to the “communications channel” between two entities that permit passing of messages through other agents and permit redirection (e.g. passing and redirecting user messages to a web service via a web browser, or any other HTTP client). See also *back channel*.

Identification

The process of recognizing an entity by contextual characteristics and its distinguishing attributes. **[X.idmdef]**

Identifier

One or more distinguishing attributes that can be used to identify an entity within a context. **[X.idmdef] [SAML-Gloss-2.0]**

Identity

- The essence of an entity [Merriam]. One's identity is often described by one's characteristics, among which may be any number of identifiers. See also Identifier, Attribute. **[SAML-Gloss-2.0]**
- A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. For identity management (IdM) purposes the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts. **[X.idmdef]**

Identity assurance

The degree of confidence in the process of identity validation and verification used to establish the identity of the entity to which the credential was issued, and the degree of confidence that the entity that uses the credential is that entity or the entity to which the credential was issued or assigned. **[X.idmdef]**

Identity defederation

The action occurring when providers agree to stop referring to a Principal via a certain set of identifiers and/or attributes. **[SAML-Gloss-2.0]**

Identity federation

The act of creating a federated identity on behalf of a Principal. **[SAML-Gloss-2.0]**

Identity management (IdM)

A set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for assurance of identity information (e.g., identifiers, credentials, attributes); assurance of the identity of an entity and supporting business and security applications. **[X.idmdef]**

Identity proofing

A process which validates and verifies sufficient information to confirm the claimed identity of the entity. **[X.idmdef]**

Identity Provider (IdP)

A kind of service provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers within a federation, such as with web browser profiles. **[SAML-Gloss-2.0]**

Identity Service Provider (IdSP)

An entity that verifies, maintains, manages, and may create and assign the identity information of other entities. **[X.idmdef]**

Login, Logon, Sign-on

The process whereby a user presents credentials to an authentication authority, establishes a simple session, and optionally establishes a rich session. **[SAML-Gloss-2.0]**

Logout, Logoff, Sign-off

The process whereby a user signifies desire to terminate a simple session or rich session. **[SAML-Gloss-2.0]**

Mutual authentication

A process by which two entities (e.g., a client and a server) authenticate each other such that each is assured of the other's identity. **[X.idmdef]**

Non-repudiation

The ability to protect against denial by one of the entities involved in an action of having participated in all or part of the action. **[X.idmdef]**

Out-of-band

A secondary communication process that provides information that supports (or may be required by) a primary communication process. The secondary process may or may not be fully defined or described as part of the primary process.

Party

Informally, one or more principals (i.e. persons or entitites) participating in some process or communication, such as receiving an assertion or accessing a resource. **[SAML-Gloss-2.0]**

Personally Identifiable Information (PII)

Any information (a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains, (b) from which identification or contact information of an individual person can be derived, or (c) that is or can be linked to a natural person directly or indirectly. **[X.idmdef]**

Policy Decision Point (PDP)

A *system entity* that makes *authorization decisions* for itself or for other system entities that request such decisions. [PolicyTerm] For example, a SAML PDP consumes authorization decision requests, and produces *authorization decision assertions* in response. A PDP is an "authorization decision authority". **[SAML-Gloss-2.0]**

Policy Enforcement Point (PEP)

A *system entity* that requests and subsequently enforces *authorization decisions*. [PolicyTerm] For example, a SAML PEP sends *authorization decision* requests to a PDP, and consumes the *authorization decision assertions* sent in response. **[SAML-Gloss-2.0]**

Principal

An entity or person whose identity can be authenticated. **[X.idmdef]**

Principal Identity

A representation of a principal's identity (e.g. a user identifier, or an identity card). A principal indentity may include distinguishing or identifying attributes.

Privacy

The right of individuals to control or influence what personal information related to them may be collected, managed, retained, accessed, and used or distributed. **[X.idmdef]**

Privacy policy

A policy that defines the requirements for protecting access to, and dissemination of, personally identifiable information (PII) and the rights of individuals with respect to how their personal information is used. **[X.idmdef]**

Privilege

A right that, when granted to an entity, permits the entity to perform an action. **[X.idmdef]**

Proofing

The verification and validation of information when enrolling new entities into identity systems. **[X.idmdef]**

Provider

A generic way to refer to both identity providers and service providers. **[SAML-Gloss-2.0]**

Proxy

An entity authorized to act for another. a) Authority or power to act for another. b) A document giving such authority. **[SAML-Gloss-2.0]**

Proxy Server

A computer process that relays a protocol between client and server computer systems, by appearing to the client to be the server and appearing to the server to be the client. **[SAML-Gloss-2.0]**

Registration

A process in which an entity requests and is assigned privileges to use a service or resource.

NOTE: Enrollment is a pre-requisite to registration. Enrollment and registration functions may be combined or separate. **[X.idmdef]**

Relying Party (RP)

- A *system entity* that decides to take an action based on information from another system entity. For example, a SAML relying party depends on receiving *assertions* from an *asserting party* (a *SAML authority*) about a *subject*. **[SAML-Gloss-2.0]**

- An entity that relies on an identity representation or claim by a requesting/asserting entity within some request context. **[X.idmdef]**

Resource

Data contained in an information system (for example, in the form of files, information in memory, etc), as well as **[SAML-Gloss-2.0] :**

1. A service provided by a system.
2. An item of system equipment (in other words, a system component such as hardware, firmware, software, or documentation).

REST, RESTful

an architectural style in software architecture for distributed hypermedia systems such as the World Wide Web. Software that conforms to the principles of REST are termed “RESTful”. Derived from **[REST-Def]**

Revocation

The annulment by someone having the authority, of something previously done. **[X.idmdef]**

Role

- Dictionaries define a role as “a character or part played by a performer” or “a function or position.” System entities don various types of roles serially and/or simultaneously, for example, active roles and passive roles. The notion of an Administrator is often an example of a role. **[SAML-Gloss-2.0]**
- A set of properties or attributes that describe the capabilities or the functions performed by an entity. NOTE: Each entity can have/play many roles. Capabilities may be inherent or assigned. **[X.idmdef]**

Security

A collection of safeguards that ensure the confidentiality of information, protect the systems or networks used to process it, and control access to them. Security typically encompasses the concepts of secrecy, confidentiality, integrity, and availability. It is intended to ensure that a system resists potentially correlated attacks. **[SAML-Gloss-2.0]**

Security architecture

A plan and set of principles for an administrative domain and its security domains that describe the security services that a system is required to provide to meet the needs of its users, the system elements required to implement the services, and the performance levels required in the elements to deal with the threat environment.

A complete security architecture for a system addresses administrative security, communication security, computer security, emanations security, personnel security, and physical security, and prescribes security policies for each.

A complete security architecture needs to deal with both intentional, intelligent threats and accidental threats. A security architecture should explicitly evolve over time as an integral part of its administrative domain’s evolution. **[SAML-Gloss-2.0]**

Security assertion

An assertion that is scrutinized in the context of a security architecture. **[SAML-Gloss-2.0]**

Security audit

An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy, and procedures. **[X.idmdef]**

Security policy

A set of rules and practices that specify or regulate how a system or organization provides security services to protect resources. Security policies are components of security architectures. Significant portions of security policies are implemented via security services, using security policy expressions. **[SAML-Gloss-2.0]**

Security service

A processing or communication service that is provided by a system to give a specific kind of protection to resources, where said resources may reside with said system or reside with other systems, for example, an authentication service or a PKI-based document attribution and authentication service. A security service is a superset of AAA services. Security services typically implement portions of security policies and are implemented via security mechanisms. **[SAML-Gloss-2.0]**

Service provider

A role donned by a system entity where the system entity provides services to principals or other system entities. Session A lasting interaction between system entities, often involving a Principal, typified by the maintenance of some state of the interaction for the duration of the interaction. **[SAML-Gloss-2.0]**

Session authority

A role donned by a system entity when it maintains state related to sessions. Identity providers often fulfill this role. **[SAML-Gloss-2.0]**

Session participant

A role donned by a system entity when it participates in a session with at least a session authority. **[SAML-Gloss-2.0]**

Subject

A principal in the context of a security domain. SAML assertions make declarations about subjects. **[SAML-Gloss-2.0]**

System Entity, Entity

An active element of a computer/network system. For example, an automated process or set of processes, a subsystem, a person or group of persons that incorporates a distinct set of functionality. **[SAML-Gloss-2.0]**

Trust

The firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context. **[X.idmdef]**

User

Any entity that makes use of a resource, e.g., system, equipment, terminal, process, application, or corporate network. **[X.idmdef]** See also *End User*.

Uniform Resource Identifier (URI)

A compact string of characters for identifying an abstract or physical resource. [RFC2396] URIs are the universal addressing mechanism for resources on the World Wide Web. Uniform Resource Locators (URLs) are a subset of URIs that use an addressing scheme tied to the resource’s primary access mechanism, for example, their network “location”. **[SAML-Gloss-2.0]**

Uniform Resource Identifier (URI), URI Reference

a compact sequence of characters that identifies an abstract or physical resource. It enables uniform identification of resources via a separately defined extensible set of naming schemes. **[RFC 3986]**

Universal Resource Locator (URL)

a compact string used for representation of a resource available via the Internet. **[RFC 1738]**

Verification

The process or instance of establishing the authenticity of something.

NOTE: Verification of (identity) information may encompass examination with respect to validity, correct source, original, (unaltered), correctness, binding to the entity, etc. **[X.idmdef]**

Verifier

An entity that verifies and validates identity information. **[X.idmdef]**

XML, eXtensible Markup Language (XML)

Extensible Markup Language (XML) is a simple, very flexible text format designed to meet the challenges of large-scale electronic publishing. XML documents provide a meaningful way to exchange a wide variety of data over networks that can be used by business, operational and other processes.

B.3 Profile Specific Definitions

Kerberos

Having to do with authentication performed by means of the Kerberos protocol as described by the IETF RFC 1510. **[RFC 1510]**

Security Assertion Markup Language (SAML)

The set of specifications describing security assertions that are encoded in XML, profiles for attaching the assertions to various protocols and frameworks, the request/response protocol used to obtain the assertions, and bindings of this protocol to various transfer protocols (for example, SOAP and HTTP).

Appendix C. Acronyms

Acronym	***Expanded Term***
2FA	Two-Factor Authentication
A2A	Application-to-Application
AAA	Authentication, Authorization and Accounting
B2B	Business-to-Business
BI	Business Intelligence
CBA	Cloud Based Application
CMDB	Configuration Management Database
COI, CoI	Community of Interest
CRM	Customer Relationship Management
CSP	Cloud Service Provider
CV	Curriculum Vitae (resume)
DIS	Domain Identity Service
DS	Delegation Service
EDI	Electronic Data Interchange
EV	Extended Validation
FI	Federated Identity or Financial Institution (depending on context)
FIM	Federated Identity Management
IdM, IDM	Identity Management
IdP, IDP	Identity Provider
IdPS	Identity Provider Service
IETF	Internet Engineering Task Force
JIT	Just-in-Time
KDC	Key Distribution Center, generally a Kerberos term.
LDAP	Lightweight Directory Access Protocol
OTP	One-Time Password
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PID	Personal ID
PIP	Policy Information Point
PKI	Public Key Infrastructure
PoU	Purpose of Use
RBAC	Role Based Access Control
REST	Representational State Transfer
SAML	Security Assertion Markup Language
SRM	Supplier Relationship Management
SSO	Single Sign-On (typically), or Single Sing-Off depending on context. Single Sign-Off is
URI	Uniform Resource Identifier
URL	Universal Resource Locator

VM	Virtual Machine
VVIP	Very, Very Important Person
XaaS	Shorthand notation indicating any “X” (variable) resource offered “as-a-Service”
XML	Extensible Markup Language