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

Cloud Authorization Use Cases Version 1.0

Committee Note Draft 01 / Public Review Draft 01

17 March 2014

Specification URIs

This version:

http://docs.oasis-open.org/cloudauthz/CloudAuthZ-usecases/v1.0/cnprd01/CloudAuthZ-usecases-v1.0-cnprd01.doc (Authoritative)
http://docs.oasis-open.org/cloudauthz/CloudAuthZ-usecases/v1.0/cnprd01/CloudAuthZ-usecases-v1.0-cnprd01.html
http://docs.oasis-open.org/cloudauthz/CloudAuthZ-usecases/v1.0/cnprd01/CloudAuthZ-usecases-v1.0-cnprd01.pdf

Previous version:

N/A

Latest version:

http://docs.oasis-open.org/cloudauthz/CloudAuthZ-usecases/v1.0/CloudAuthZ-usecases-v1.0.doc (Authoritative)
http://docs.oasis-open.org/cloudauthz/CloudAuthZ-usecases/v1.0/CloudAuthZ-usecases-v1.0.html
http://docs.oasis-open.org/cloudauthz/CloudAuthZ-usecases/v1.0/CloudAuthZ-usecases-v1.0.pdf

Technical Committee:

OASIS Cloud Authorization TC

Chairs:

Anil Saldhana (anil.saldhana@redhat.com), Red Hat, Inc.
Radu Marian (radu.marian@baml.com), Bank of America

Editors:

Anil Saldhana (anil.saldhana@redhat.com), Red Hat, Inc.
Radu Marian (radu.marian@baml.com), Bank of America
Felix Gomez Marmol (felix.gomez-marmol@neclab.eu), NEC Corporation
Chris Kappler (chris.kappler@pwc.be), PricewaterhouseCoopers LLC

Abstract:

This document is intended to provide a set of representative use cases that examine the requirements on Cloud Authorization 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 Cloud Authorization 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 https://www.oasis-open.org/committees/cloudauthz/.

Citation format:

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

[CloudAuthZ-Usecases]

Cloud Authorization Use Cases Version 1.0. Edited by Anil Saldhana, Radu Marian, Felix Gomez Marmol, and Chris Kappler. 17 March 2014. OASIS Committee Note Draft 01 / Public Review Draft 01. http://docs.oasis-open.org/cloudauthz/CloudAuthZ-usecases/v1.0/cnprd01/CloudAuthZ-usecases-v1.0-cnprd01.html. Latest version: http://docs.oasis-open.org/cloudauthz/CloudAuthZ-usecases/v1.0/CloudAuthZ-usecases-v1.0.html.

WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

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 Cloud Authorization TC is to collect use cases to help identify gaps in existing Cloud Authorization standards. The use cases will be used to identify gaps in current standards and investigate the definition of entitlements.

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 its 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
  - General Authorization
  - Administration
- 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.

2.2.4.1 General Authorization

This category is used if the use case features the need for authorization in general terms without specifying or referencing particular methods or patterns.

2.2.4.2 Administration

This category is used if the use case features the need for the administration of access control policies.

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.

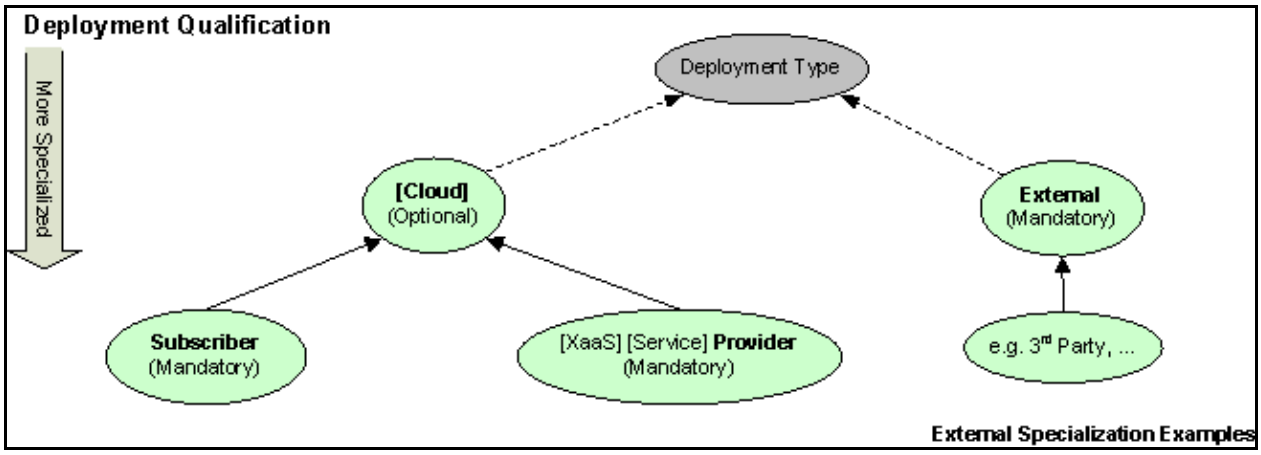
The general syntax for creating a name for an actor is as follows:

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.

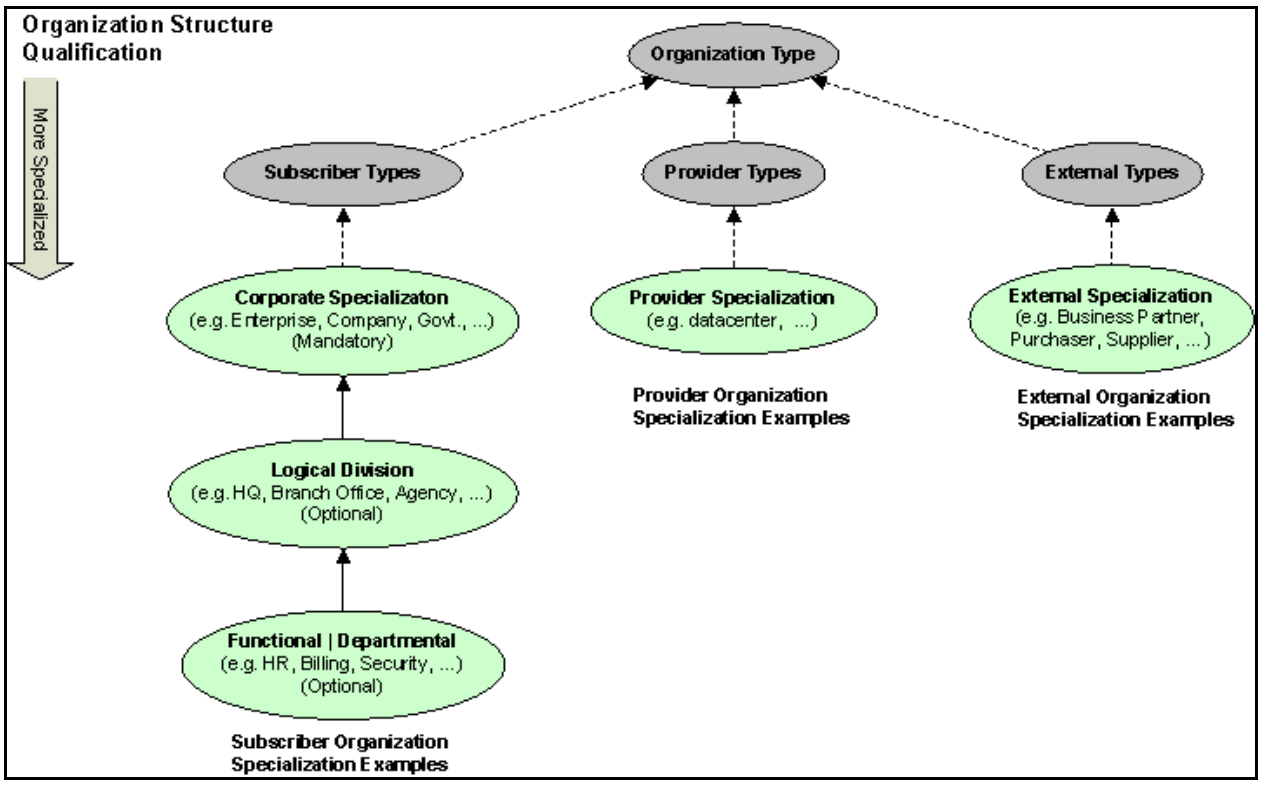
2.3.1 Deployment Qualifications

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



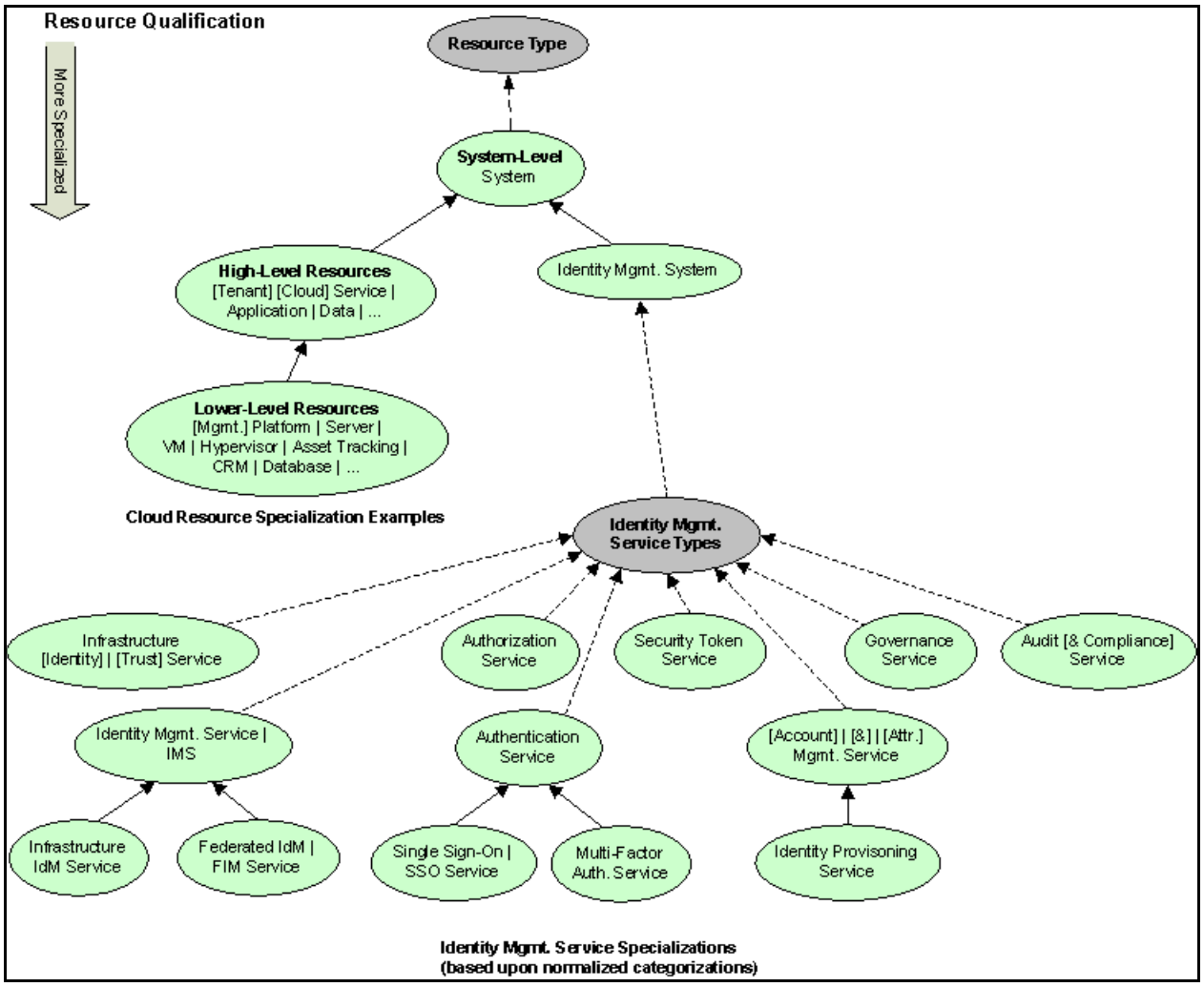
2.3.2 Organization Qualifications

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



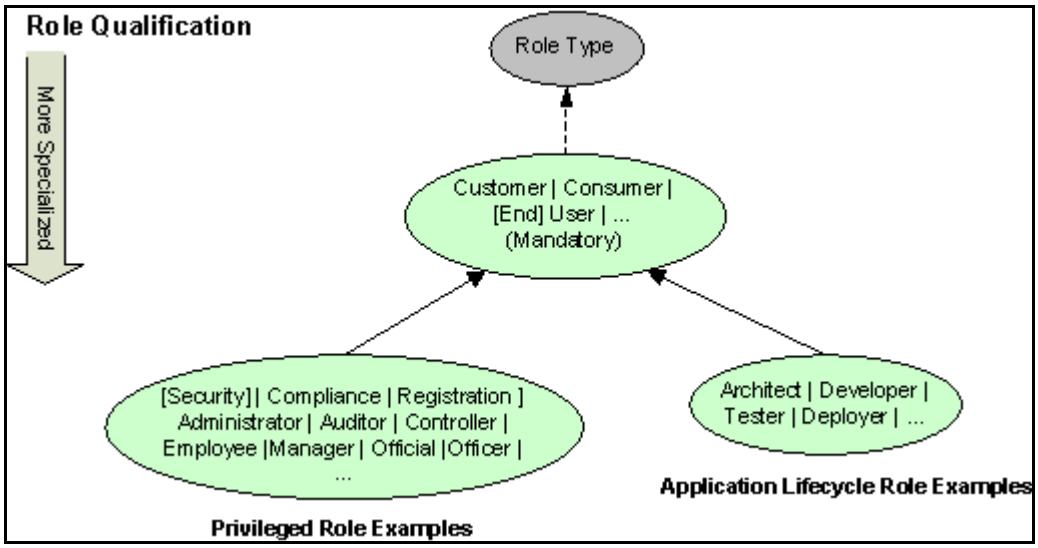
2.3.3 Resource Qualifications

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:



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	Context Driven Entitlements	Entitlements or permissions of a subject during an access decision check can be obtained from a repository or service.
2	Attribute and Provider Reliability Indexes	The policy author is able to define a policy that allows for the real-time assessment of the reliability of an attribute provider or the individual reliability for any attribute it provides. This allows for varying levels of access control policy to be applied dependent on the value of the reliability index retrieved for the provider and/or its attributes. When reliability is low, the policy author defines more approval/controls and less access for the same decision matrix, applied to the same set of identity attributes. This should allow for better decisions to be made.
3	Entitlements Catalog	Entitlements Catalog is a service that returns a list of Business Tasks a user can perform.
4	Segregation of Duties based on Business Process	A Segregation of Duties service that uses Business Process, Activity, and Task as defined by Business Architects to represent the Duties and potential conflicting entitlements.
5	Employing a “Reliability Index” in federated policy decision flows	“Reliability Index” will help providers and consumers define, model and understand an integrity rating for a given attribute, set of attributes or attribute provider having the goal of creating meaningful access policies, policies that reflect the dependencies, reliability and overall risks inherent in the authorization system as a whole.
6	Distributed Authorization	For authorization decisions that depend on the information belonging to other domains, which cannot be directly accessed due to privacy issues instead of recovering the required information, the authorization decision is delegated

Use Case #	Title	Goals Description Comments
		to the areas which could handle it, and the results of such delegated decisions are combined to form an appropriate decision.
7	Administrate distributed access control policies	Allow subsidiaries to implement their own policies where applicable but use a set of common policies for all (or a sub-set) of subsidiaries.
8	Authorization audit	Cloud Authorization services perform access control decision on sensitive data. There is a need to log and audit the output and details of the authorization decision performed to trace the relevant events happened in the system.
9	Risk based access control systems	Cloud Authorization services may determine access based on a computation of security risk and operational need, not just proper comparison of attributes. In other words, for each Risk Level and kind of resource, a set of specific counter-measures to protect the resource has to be triggered. Moreover, this risk level could vary during the time, so they should adapt to different situation.
10	Policies to determine administration privileges	The administrator of authorization systems usually specifies the access privileges by defining access control policies. Administrative policies are necessary to control the administrators/special-users who modify the access control policies. This is especially relevant in scenarios where administrator could define policies outside its domain, for instance in distributed systems.
11	Delegate privileges	Cloud Authorization Service may provide administration capabilities to the Cloud Users so they could define certain delegation policies that want to temporary delegate some of access rights to another Cloud User, without directly involving the policies Administrator.
12	Enforce government access control decisions	To be able to assure tenants' compliance and security government access control policies need to be created, consistently managed and enforced. The authorization decisions may need to be governed or managed by geographical locations to enforce regional and national compliance policies.

4 Use Cases

4.1 Use Case 1: Context Driven Entitlements

4.1.1 Description / User Story

In a Cloud Computing Environment, access decisions need to be made based on the context. The context includes the subject, the resource, the action, the environment and attributes of each of these. Access Decisions can be made if entitlements or permissions the subject has can be obtained.

4.1.2 Goal or Desired Outcome

`Entitlements or permissions of a subject during an access decision check can be` obtained from a repository or service.

4.1.3 Notable Categorizations and Aspects

Categories Covered:
• Primary
  ○ Authorization.
  ○ Account and Attribute Mgmt. (Provisioning).
• Secondary:
  ○ Audit and Compliance.
	Featured Deployment and Service Models:
	• Deployment Models
	  ○ Private
	  ○ Public
	• Service Models
	  ○ Platform-as-a-Service (PaaS)
	  ○ Infrastructure-as-a-Service (IaaS)

Actors: • Cloud User • Cloud Resource	**Systems:** • Cloud Provider Identity Mgmt. System, helps manage resources such as: • Cloud Identity Stores
Notable Services: • Cloud Authentication Service • Cloud Authorization Service • Cloud Entitlement Service	
Dependencies: • None	
Assumptions: • Entitlements or permissions for a subject are stored in a repository or can be obtained from an external service.	

4.1.4 Process Flow

1. A Cloud User tries to access a Cloud Resource.
2. The Cloud Authorization Service tries to determine if the Cloud User has access to the Cloud Resource.
3. The Cloud Authorization Service needs the permissions or the entitlements the Cloud User has. It asks a Cloud Entitlement Service for the permissions or entitlements the Cloud User has for the particular Cloud Resource, for the particular action and the environment such as IP Address, DateTime etc.
4. The Cloud Entitlement Service returns a set of permissions. The Cloud Authorization Service does the access check based on the entitlements.

4.2 Use Case 2: Attribute and Provider Reliability Indexes

4.2.1 Description / User Story

When designing a policy within a federated authorization system, the policy designer places a high degree of overall system integrity in the 'quality" of the attributes used in a given policy decision. The active exchange of attributes and data between relying parties in distributed cloud / federated authorization systems, makes it hard to design policies that allow for the varying levels of controls & assurance placed around attribute management lifecycle controls.

This user story introduces the use of a "reliability index" to help providers and consumers define, model and understand an integrity rating for a given attribute, set of attributes or attribute provider By employing a reliability index for the attribute provider and for the specific attributes it provides, the policy designer is able to create more meaningful access policies, policies that reflect the dependencies, reliability and overall risks inherent in the authorization system as a whole.

4.2.2 Goal or Desired Outcome

The policy author is able to define a policy that allows for the real-time assessment of the reliability of an attribute provider or the individual reliability for any attribute it provides. This allows for varying levels of access control policy to be applied dependent on the value of the reliability index retrieved for the provider and/or its attributes. When reliability is low, the policy author defines more approval/controls and less access for the same decision matrix, applied to the same set of identity attributes. This should allow for better decisions to be made.

4.2.3 Notable Categorizations and Aspects

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

• Primary
  ○ General Identity Mgmt.
  ○ Account and Attribute Mgmt.
	• Deployment Models
	  ○ None featured
	• Service Models

• Secondary ○ None	○ 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: Entitlements Catalog

4.3.1 Description / User Story

Company "A" wishes to use services provided by a cloud service provider. There is a strong need to know what entitlements User has during Entitlement Assignment, Provisioning, Access Runtime, and Access Review phases of IAM.

Entitlements Catalog service returns a list of Business Tasks a user can perform. Entitlements should be portable from one service provider to another.

4.3.2 Goal or Desired Outcome

At any point in time it should be possible to find out what entitlements user has.

Since Entitlements are to be portable from one CSP to another:

1. User entitlements should not be system specific but rather be based on Business Tasks as defined by business architects

2. User entitlements should be expressed in a standard format that is based on a pre-defined and agreed upon access control vocabulary that enables one to express entitlements syntax as well as entitlement meaning.

4.3.3 Notable Categorizations and Aspects

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

• Standard Entitlements Model
  ○ Entitlements Semantics
  ○ Entitlements Portability
• Entitlement Assignment
• User Provisioning
• Runtime Authorization
• Access Review
	• Cloud Deployment Models
	  ○ Public
	  ○ Private
	• Service Models
	  ○ Infrastructure-as-a-Service (IaaS)

Actors: • Entitlements Manager • Business Architect • Access Reviewer • User	**Systems:** • Enterprise • Cloud Service Provider • Entitlement Model Repository

Notable Services:
• User Entitlement Management Services:
  ○ GetUserEntitlements – retrieve User entitlements.
  ○ GetEntitlementSyntax – retrieve Entitlement Type Syntax.
  ○ GetEntitlementMeaning – retrieve the meaning of the particular entitlement.	

Dependencies: • An Access Control Vocabulary exists to provide syntax and meaning for each entitlement. • CSPs agree to use the above Access Control Vocabulary to express entitlements in a portable format.	
Assumptions: • Business Process Framework is provided as input to the Entitlements Model.	

4.3.4 Process Flow

The process flow is as follows:

- A company uses the services provided by the Cloud Service Provider.
- The Cloud Service Provider exposes various services representing entitlements for the users from the company.
- The company calls GetUserEntitlements service to receive a list of entitlements for a particular user.
- The company calls GetEntitlementSyntax service to receive the syntax of an entitlement.

- The company calls GetEntitlementMeaning service to receive the meaning a particular entitlement.

4.4 Use Case 4: Segregation of Duties based on Business Process

4.4.1 Description / User Story

A company for whom a CSP is providing services needs to implement corresponding Segregation of Duties Policies. There is a strong need to know what conflicting entitlements a user could be assigned, prevent such assignment, augment the conflicting assignment with runtime controls, and as a last resort detect the use of conflicting entitlements.

4.4.2 Goal or Desired Outcome

Provide a policy-based mechanism to design, implement, test, and access review simple and complex Separation of Duties scenarios.

Leverage XACML standard for expressing the conditional logic of SoD policies. Leverage Access Control Vocabulary to express the syntax and meaning of attributes used in SoD Policies.

Business Tasks is to be the core attribute for designing and registering "Duties" of Segregation of Duties.

4.4.3 Notable Categorizations and Aspects

<table>
<tr>
<td>Categories Covered:
Entitlement Semantic Model
Entitlement Assignment
Runtime Authorization
Access Review</td>
<td>Applicable Deployment and Service Models:
Cloud Deployment Models
Public
Private
Service Models
Infrastructure-as-a-Service (IaaS)</td>
</tr>
<tr>
<td>Actors:
Business Architect
Entitlements Designer
Entitlements Manager
Access Reviewer
User</td>
<td>Systems:
Enterprise
Cloud Service Provider
Entitlement Model Repository</td>
</tr>
<tr>
<td colspan="2">Notable Services:
User Entitlement Management Services:
GetUserEntitlements – retrieve User entitlements.
FindConflictingEntitlements – for a given number of entitlements list conflicting entitlements</td>
</tr>
</table>

Dependencies:
• Access Control Vocabulary exist to provide syntax and meaning for each entitlement. • CSPs agree to use the above Access Control Vocabulary to express entitlements in a portable format.
Assumptions:
• Business Process Framework is provided as input to the Entitlements Model.

4.4.4 Process Flow

N/A

4.5 Use case 5: Employing a "Reliability Index" in federated policy decision flows

4.5.1 Description/User Story

When designing a policy within a federated authorization system, the policy designer places a high degree of overall system integrity in the 'quality" of the attributes used in a given policy decision. The active exchange of attributes and data between relying parties in distributed cloud / federated authorization systems, makes it hard to design policies that allow for the varying levels of controls & assurance placed around attribute management lifecycle controls.

This user story introduces the use of a "reliability index" to help providers and consumers define, model and understand an integrity rating for a given attribute, set of attributes or attribute provider By employing a reliability index for the attribute provider and for the specific attributes it provides, the policy designer is able to create more meaningful access policies, policies that reflect the dependencies, reliability and overall risks inherent in the authorization system as a whole.

4.5.2 Goal or Desired Outcome

The policy author is able to define a policy that allows for the real-time assessment of the reliability of an attribute provider or the individual reliability for any attribute it provides. This allows for varying levels of access control policy to be applied dependent on the value of the reliability index retrieved for the provider and/or its attributes. When reliability is low, the policy author defines more approval/controls and less access for the same decision matrix, applied to the same set of identity attributes. This should allow for better decisions to be made.

4.5.3 Applicable Deployment and Service Models

This user story applies to the following cloud deployment and service models

4.5.3.1 Cloud Deployment Models:

Private, Public, Community, Hybrid Service Models, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS)

4.5.4 Actors

4.5.4.1 The Attribute Authority

The logical entity that provides an attribute for use in the evaluation of a policy.

4.5.4.2 The Policy Author

The author or creator of a given access authorization decision policy.

4.5.4.3 The Policy Decision Point

The logical entity that makes policy decisions for itself or for other network elements that request such decision.

4.5.5 Systems

N/A

4.5.6 Notable Services

N/A

4.5.7 Assumptions

An operating trust model exits within a federated access authorization system. The overall system is appropriately configured to allow for policy decision flows in accordance with the use case.

4.5.8 Process Flow

The POLICY_AUTHOR writes a policy that only provides access to PROTECTED_RESOURCE if the SPECIFIC _SUBJECT is OVER_21.

The ATTRIBUTE_PROVIDER asserts that SPECIFIC_SUBJECT is over 21 and carries out a physical driving license inspection and an in person interview. ATTRIBUTE_PROVIDER places a very high ATTRIBUTE_RELIABIITY_INDEX to its OVER_21 attribute due to its strong internal control procedures.

In this case, the ATTRIBUTE_PROVIDER is awarded a high PROVIDER_RELIABIITY_INDEX because it is the Texas DMV and is the actual issuer of the driving license in question.

When OVER_21 is true and either of the ATTRIBUTE_RELIABIITY_INDEX or the PROVIDER_RELIABIITY_INDEX are high, the SPECIFIC_SUBJECT is provides direct access to PROTECTED_RESOURCE. If either the ATTRIBUTE_RELIABIITY_INDEX or the

PROVIDER_RELIABIITY_INDEX are not high, then SPECIFIC_SUBJECT is asked to confirm their age before being provided access to PROTECTED_RESOURCE.

4.6 Use case 6: Distributed Authorization

4.6.1 Description/User Story

Enterprises and corporations are usually composed of different working areas or departments: human resources, operations, business office, administrative office, etc. Each corporate area may implement its own access control rules that handle the information and resources in their respective areas and are, somehow, enforcement points.

However, some authorization decisions may depend on the information belonging to other areas or domain, which cannot be directly accessed due to privacy issues. In this sense, instead of recovering the required information, the authorization decision is delegated to the areas that could handle it, and the results of such delegated decisions are combined to form an appropriate decision.

4.6.2 Goal or Desired Outcome

Authorization decisions are taken based on the decisions of multiples cloud computing parties.

4.6.3 Categories Covered

- Authorization.
- Account and Attribute management.

4.6.4 Applicable Deployment and Service Models

- All Cloud Deployment Models (Private, Public, Community and Hybrid).
- All Service Models (SaaS, PaaS and IaaS).

4.6.5 Actors

- Cloud user.
- Cloud Resource.
- Local Policy Decision Point
- External Policy Decision Point
- External Attribute Authority

4.6.6 Systems

N/A

4.6.7 Notable Services

- Cloud Authorization Service
- Cloud Entitlement Service

4.6.8 Dependencies

N/A

4.6.9 Assumptions

Access control policies are deployed among different administrative domains or areas. Each area deploys policies related to the information they manage.

4.6.10 Process Flow

A Cloud User belonging to the administrative domain A tries to access a Cloud Resource controlled by the administrative domain B. To determine if the Cloud User has access to the Cloud Resource, the authorization policies of both domain A (e.g. only users with a specific role could access to external resources) and B (e.g. only users belonging to a specific domain could access to the given Cloud Resource) have to be evaluated. The Policy Decision Point of the domain B evaluates its policies and it requests the Policy Decision Point of the domain A for its authorization decision. The decision from the domain A is combined with its own policies to form the final authorization decision.

4.7 Use case 7: Administrate distributed access control policies

4.7.1 Description/User Story

Large corporations are usually composed of a central office and multiple subsidiaries. We may consider that the central office and each of its subsidiaries independently implement an authorization architecture with their own access policies to manage their resources.

The central office will need to have an appropriate management over the access control policies of the subsidiaries, in order to establish, for instance, a set of common policies for all subsidiaries (depending for example on some mandatory corporate regulations) or to assign specific policies to each one (depending for example on the type of service they provide), but at the same time allowing that each subsidiary implement its own policies.

4.7.2 Goal or Desired Outcome

An administrative domain could manage policies in other administrative domains in a controlled way.

4.7.3 Categories Covered

- Account and Attribute management.
- Policies Management
- Authorization

4.7.4 Applicable Deployment and Service Models

- All Cloud Deployment Models (Private, Public, Community and Hybrid).
- All Service Models (SaaS, PaaS and IaaS).

4.7.5 Actors

- Policies Administrator

4.7.6 Systems

N/A

4.7.7 Notable Services

- Cloud Authorization Service
- Policy Administration Service

4.7.8 Dependencies

This use case may depend on Use Case 1.

4.7.9 Assumptions

An administrative domain has the appropriate privileges to write authorization policies in other administrative domains.

4.7.10 Process Flow

A Policies Administrator belonging to a given administrative domain wants to spread access control policies to other administrative domains in order to be enforced by them.

4.8 Use case 8: Authorization audit

4.8.1 Description/User Story

Cloud Authorization Services perform access control decision on sensitive data. There is a need to log and audit the output and details of the authorization decision performed to trace the relevant events happened in the system.

4.8.2 Goal or Desired Outcome

Trace the relevant events happened in the system. Cloud User or entities cannot deny having performed an operation or initiated a transaction.

4.8.3 Categories Covered

- Audit and Compliance

4.8.4 Applicable Deployment and Service Models

- All Cloud Deployment Models (Private, Public, Community and Hybrid).
- All Service Models (SaaS, PaaS and IaaS).

4.8.5 Actors

- Policy Decision Point

4.8.6 Systems

N/A

4.8.7 Notable Services

- Cloud Authorization Service
- Cloud Audit Service

4.8.8 Dependencies

N/A

4.8.9 Assumptions

N/A

4.8.10 Process Flow

A Cloud Authorization Service evaluates some authorization policies to resolve an authorization query. The query, the decision and other relevant details of the evaluation are stored in logs files in either an internal or external service. Additionally, the logs are signed to provide non-repudiation capabilities.

4.9 Use case 9: Risk based access control systems

4.9.1 Description/User Story

Traditional access control systems assume uniformity of people, components, environments, conditions, etc. across the scenario and time. They tend to define its behavior based on static policies. However, when moving to the cloud, they should consider multiple factors to determine the security risk and operational need of each access decision.

Cloud Authorization services may determine access based on a computation of security risk and operational need, not just proper comparison of attributes. In other words, for each Risk Level and kind of resource, a set of specific counter-measures to protect the resource has to be triggered. Moreover, this risk level could vary during the time, so they should adapt to different situation.

4.9.2 Goal or Desired Outcome

Define and adapt enterprise policies for establishing thresholds for security risk and operational need under various conditions

4.9.3 Categories Covered

- Policies Management

4.9.4 Applicable Deployment and Service Models

- All Cloud Deployment Models (Private, Public, Community and Hybrid).
- All Service Models (SaaS, PaaS and IaaS).

4.9.5 Actors

- Cloud User
- Cloud Resource
- Policy Decision Point

4.9.6 Systems

N/A

4.9.7 Notable Services

- Risk Level Administrator Service

4.9.8 Dependencies

N/A

4.9.9 Assumptions

The authorization policies could be defined based on security risk levels.

4.9.10 Process Flow

A Cloud User wants to perform an operation over a Cloud Resource. To determine if the Cloud User is able to do it, an authorization decision is achieved based on the level of risk of the operation on this resource at that specific moment.

4.10 Use case 10: Policies to determine administration privileges

4.10.1 Description/User Story

An administrator of authorization systems usually specifies the access privileges by defining access control policies. Administrative policies are necessary to control the administrators/special-users who modify the access control policies. This is especially relevant in scenarios where administrator could define policies outside its domain, for instance in distributed systems.

4.10.2 Goal or Desired Outcome

Policies to determine administration privileges are evaluated before the administrator could modify the access control policies.

4.10.3 Categories Covered

- Authorization
- Policies Management
- Account and Attribute Management

4.10.4 Applicable Deployment and Service Models

- All Cloud Deployment Models (Private, Public, Community and Hybrid).
- All Service Models (SaaS, PaaS and IaaS).

4.10.5 Actors

- Policies administrator
- Policy Decision Point

4.10.6 Systems

N/A

4.10.7 Notable Services

- Cloud Policy Administration Service

4.10.8 Dependencies

N/A

4.10.9 Assumptions

N/A

4.10.10 Process Flow

A Policy Administrator tries to change some policies either in an internal or external administrative domain. To determine if the administrator is able to change these policies, a Policy Decision Point firstly evaluates the administrative-policies, which determine the privileges of the administrators.

4.11 Use case 11: Delegate privileges

4.11.1 Description/User Story

In some Cloud scenarios it is common that a Cloud User that holds certain privileges wants to temporary delegate some of them to another Cloud User, without directly involving the policies Administrator. For instance, a Cloud User may want to transfer their role to other Cloud User to perform a specific action, such as a PhD advisor wanting to delegate their privileges to access a digital library to one of their PhD student.

The Cloud Authorization Service may provide administration capabilities to the Cloud Users so they could define certain delegation policies, ideally in a user-friendly way.

4.11.2 Goal or Desired Outcome

Cloud users are able to temporary delegate part of their privileges to other Cloud users dynamically by making use a special policy administration service.

4.11.3 Categories Covered

- Authorization
- Account and Attribute Management

4.11.4 Applicable Deployment and Service Models

- All Cloud Deployment Models (Private, Public, Community and Hybrid).
- All Service Models (SaaS, PaaS and IaaS).

4.11.5 Actors

- Cloud User
- Policy Decision Point

4.11.6 Systems

N/A

4.11.7 Notable Services

- Cloud Policy Administration Service
- Cloud Authorization Service

4.11.8 Dependencies

N/A

4.11.9 Assumptions

N/A

4.11.10 Process Flow

A Cloud User has certain privileges to access a given Cloud Resource. The Cloud User accesses a Cloud Policy Administration Service to define its own delegation policies. These policies specify the conditions of the delegation, such as targeted subjects, time of applicability, environments circumstances, etc. Another Cloud User tries to access the Cloud Resource. The Policy Decision Point evaluates their policies together with the delegation policies to determine whether the Cloud User has access to the Cloud Resource. The Cloud User will have access to the resource if it has the appropriate privileges required for accessing to that resource, or if such privileges have been delegated from other Cloud User.

4.12 Use case 12: Enforce government access control decisions

4.12.1 Description/User Story

Cloud service providers tend to manage their authorization services by defining their own policies and rules according to their business requirements. However, regional and national governments have their own requirements.

Cloud service providers should be able to assure that tenants' compliance and security policies are consistently managed and enforced. The authorization decisions may need to be governed or managed by geographical locations to enforce regional compliance policies.

An issue we should not neglect as well is how enterprises or organizations offering services on the Cloud can ensure compliance with the laws and regulations that they are subject to.

4.12.2 Goal or Desired Outcome

Authorization decisions comply with applicable laws and regulations.

4.12.3 Categories Covered

- Authorization
- Audit and Compliance
- Governance

4.12.4 Applicable Deployment and Service Models

- All Cloud Deployment Models (Private, Public, Community and Hybrid).
- All Service Models (SaaS, PaaS and IaaS).

4.12.5 Actors

- Policy Decision Point
- Government Authority

4.12.6 Systems

N/A

4.12.7 Notable Services

- Cloud Policy Administration Service
- Cloud Authorization Service

4.12.8 Dependencies

N/A

4.12.9 Assumptions

N/A

4.12.10 Process Flow

A Cloud User wants to access a Cloud Resource. The Policy Decision Point that evaluates the access control policies related to that Cloud Resource has to take into account applicable regulations to decide whether the Cloud User has access.

Appendix A. Acknowledgments

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

Chairs

Anil Saldhana, Red Hat

Radu Marian, Bank Of America

Editors

Anil Saldhana, Red Hat

Radu Marian, Bank Of America

Chris Kappler, Pricewaterhousecoopers

Dr.Felix Gomez Marmol, NEC Corporation

Document Contributors:

Abbie Barbir, Individual

Anil Saldhana, Red Hat

Darran Rolls, SailPoint

Gines Dolera Tormo, NEC Corporation

Technical Committee Member Participants:

Abbie Barbir (Bank of America)

Radu Marian (Bank of America)

Anil Saldhana (Red Hat)

Shaheen Abdul Jabbar, (JP Morgan Chase)

Darran Rolls (Sailpoint)

Chris Kappler (Pricewaterhousecoopers)

Dale Moberg (Axway)

Danny Thorpe (Dell)

Mohammad Jafari (Veterans Health Administration)

Mark Lambiase (SecureAuth)

Gene Myers (Certivox)

Andrew Innes (Citrix)

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 that 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. This includes the inability to trace the name or identity by behavior, frequency of service usage or physical location among other things. **[SAML-Gloss-2.0]**

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. 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). **[SAML-Gloss-2.0]**

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). 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. **[SAML-Gloss-2.0]**

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 entity 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. An example would be an HTTP client (e.g. a user agent) communicating directly to a web service. See also *front channel*. **[SAML-Gloss-2.0]**

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 behavioral 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 that 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 entities) 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 identity 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

Appendix D. Revision History

Revision	Date	Editor	Changes Made
1.0 a	April 15, 2013	Anil Saldhana	• Initial Version with content from OASIS IDCloud Use Case Document v1.0
1.0c	May 13, 2013	Radu Marian	• Fixed formatting • Use Cases from emails and TC Meetings
1.0d	June 10, 2013	Anil Saldhana	• Content corrections based on TC Meetings
1.0e	Nov 25, 2013	Anil Saldhana	• Spell Check
1.0f	Nov 25,2013	Anil Saldhana	• Fixed styles and formatting • Added subcategories for Authorization
1.0g	Nov26, 2013	Anil Saldhana	• Added subcategories for Authorization
1.0h	Nov 27, 2013	Chris Kappler	• Fixed styles and formatting for the appendixes • Cosmetic changes • Replaced TBD by N/A

