SailPoint Technologies

OASIS Cloud ID Technical Committee Use Case Submission

Author	Darran Rolls, SailPoint Technologies
Doc Version	003

Last Changed Date	04/18/2011
Change Summary	third release of the Cloud ID use cases from SailPoint Technologies. Changes /streamlined language and added process flow diagrams

Index

1. Use Case One: Describe Entitlement Model

1.1. Description/User Story

1.1.1. 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 an externalization of the entitlement model so that it may be reviewed, audited and document by a third party.

1.1.2. The provider may choose to externalize its entitlement model in a variety of documentation formats one of which should be a pre agreed upon structured XML document schema.

1.2. **Goal or Desired Outcome**

1.2.1. A goal of this use case is to enable external audit, governance and management services to collect a detailed understanding of what authorization, security and entitlement capabilities are available for assignment to accounts and identities within the application
1.2.2. A goal of this use case is to enable external management systems to define external encapsulations (roles or managed attributes) that can be used to control account and entitlement provisioning activities
1.2.3. A goal of this use case is to enable external management systems to create documentation and management facilities that detail what a given authorization or entitlement gives entitlement to (targets and permissions data). An example would be provider "P1" listing entitlement "A" as being available for application "App1" and further detailing it as entitling access to application functions "f1, f2 & f3"
1.2.4. A goal of this use case is to enable external management services to create entitlement glossaries/dictionaries/metadata repositories for available entitlements as part of an identity governance initiative

1.3. Categories Covered

1.3.1. TBD

1.4. **Deployment and Service Models**

1.4.1. This use case applies to the following cloud service models

1.4.1.1. Cloud Deployment Models
1.4.1.1.1. Private
1.4.1.1.2. Public
1.4.1.1.3. Community
1.4.1.1.4. Hybrid

1.4.1.2. Service Models
1.4.1.2.1. Software-as-a-Service (SaaS)
1.4.1.2.2. Platform-as-a-Service (PaaS)

1.5. **Actors**

1.5.1. The following actors take part in this use case
1.5.1.1. Cloud Based Application (CBA)
1.5.1.2. External Identity Governance Application (IGA)

1.6. **Systems**

1.6.1. TBD

1.7. **Notable Services**

1.7.1. It is assumed that the Cloud Based Application Provider makes available a remote API or requestable service point that facilitates a request/response protocol for the collection of defined entitlement models
1.7.2. The remote API or requestable service point 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

1.8. **Dependencies**

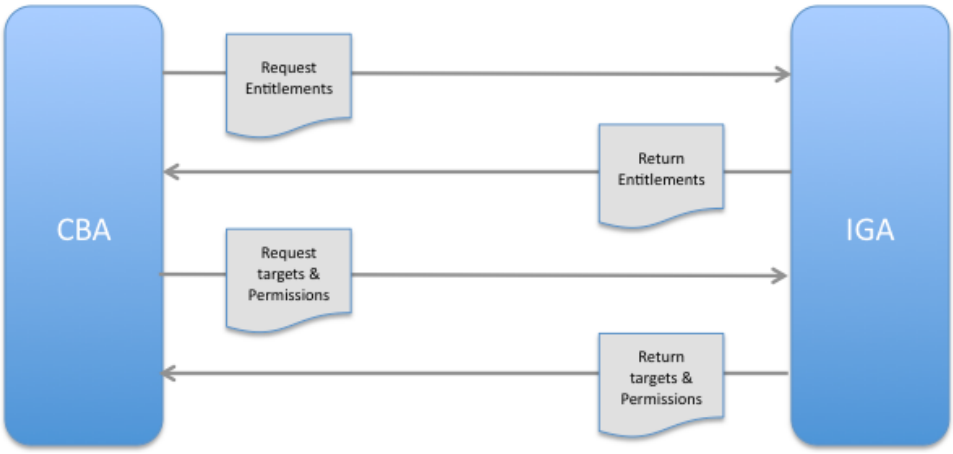
1.8.1. TBD

1.9. **Assumptions**

1.9.1. TBD

1.10. **Process Flow**

1.10.1. Overview Process Flow (figure 1)



1.10.2. The external Identity Governance Application (IGA) contacts the Cloud Based Application (CBA) and establishes a secure connection (not shown in figure 1)

1.10.3. The IGA requests an export of the assignable entitlement model for a given application

1.10.4. The CBA creates a well formed XML document export of the assignable entitlement model and returns it to the calling IGA

1.10.5. The IGA then requests an export of available target and permissions data available for a given assignable entitlement

1.10.6. The CBA creates a well formed XML document export of the available target and permissions data for the specified entitlement and returns it to the calling IGA

2. Use Case Two: List Accounts & Entitlement Assignments

2.1. **Description/User Story**

2.1.1. 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 documentation that describes the user accounts it maintains and provide details of entitlement model assignment

2.1.2. The provider may choose to externalize its account and entitlement assignment model in a variety of documentation formats one of which should be a pre agreed upon structured XML document schema.

2.1.3. This use case is differentiated from similar “read operation” use cases presented around general account and identity provisioning as it may be provided without any of the expected “write” capabilities that usually come with a remote provisioning service / capability and implemented with the focus on volume read operations and the simplicity of interpretation of the returned results. In short its read optimized.

2.2. **Goal or Desired Outcome**

2.2.1. The goal of this use case is to enable external management services the ability to collect a detailed understanding of all accounts and entitlement assignments being used within a providers application

2.3. Categories Covered

2.3.1. TBD

2.4. Deployment and Service Models

2.4.1. This use case applies to the following cloud service models

2.4.1.1. Cloud Deployment Models
- 2.4.1.1.1. Private
- 2.4.1.1.2. Public
- 2.4.1.1.3. Community
- 2.4.1.1.4. Hybrid

2.4.1.2. Service Models
- 2.4.1.2.1. Software-as-a-Service (SaaS)
- 2.4.1.2.2. Platform-as-a-Service (PaaS)

2.5. Actors

2.5.1. The following actors take part in this use case
- 2.5.1.1. Cloud Based Application (CBA)
- 2.5.1.2. External Identity Governance Application (IGA)

2.6. Systems

2.6.1. TBD

2.7. Notable Services

2.7.1. It is assumed that the Cloud Based Application (CBA) or its provider provides a remote API or requestable service point that facilitates the request/response protocol for the collection of the defined account and entitlement assignments

2.8. Dependencies

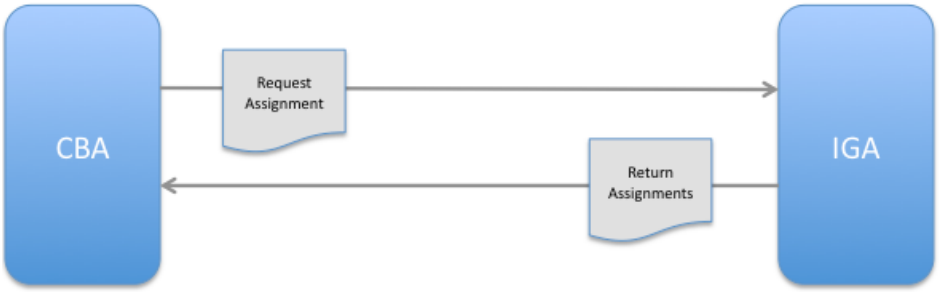
2.8.1. TBD

2.9. Assumptions

2.9.1. TBD

2.10. Process Flow

2.10.1. Process Flow Overview (figure 2)



2.10.2. The external Identity Governance Application (IGA) contacts the Cloud Based Application (CBA) and establishes a secure connection (not shown in figure 2)

2.10.3. The IGA requests an export of the account and entitlement assignment model for a given application

2.10.4. The CBA creates a well formed XML document export of the accounts and assigned entitlement model and returns it to the calling IGA

3. Use Case Three: Governance Based Provisioning

3.1. Description/User Story

3.1.1. 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 a general provisioning API (or service point) that enables external management applications to query, create, update and delete accounts and entitlement assignments to accounts and entitlement assignments that it controls. In general this use case does not differentiate between batch and singleton provisioning requests.

3.1.2. This use case include the provisioning of application level end-user accounts & entitlements and the ability to manage accounts & entitlements within the supporting infrastructure for the application

3.1.3. This use case includes a notification service that allows for the notification of changes carried out via other local or remote provisioning services (for example a Just In Time Provisioning (JIT-P) action). This use case enables an external management applications to track changes made to the identity or its entitlement assignments using this notification service.

3.1.4. This use case 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 for the purpose of enhanced Identity and Access Governance

3.2. Goal or Desired Outcome

3.2.1. A goal of this use case is to enable external management services to interact with cloud-based applications to create, update and delete accounts and entitlement assignments to those accounts and or its supporting infrastructre.

3.3. Categories Covered

3.3.1. TBD

3.4. Deployment and Service Models

3.4.1. This use case applies to the following cloud service models

3.4.1.1. Cloud Deployment Models
3.4.1.1.1. Private
3.4.1.1.2. Public
3.4.1.1.3. Community
3.4.1.1.4. Hybrid

3.4.1.2. Service Models
3.4.1.2.1. Software-as-a-Service (SaaS)
3.4.1.2.2. Platform-as-a-Service (PaaS)
3.4.1.2.3. Infrastructure-as-a-Service (IaaS)

3.5. Actors

3.5.1. The following actors take part in this use case
3.5.1.1. Cloud Based Application (CBA)
3.5.1.2. External Identity Governance Application (IGA)

3.6. Systems

3.6.1. TBD

3.7. Notable Services

3.7.1. It is assumed that the Cloud Based Application (CBA) or its provider enables a remote API or requestable service point that facilitates the request/response protocol for the provisioning actions listed in this use case

3.7.2. The remote API or requestable service point that facilitates the request/response protocol for the collection of the defined account and assigned entitlement model may be provided by an external application proxy or provider

3.8. Dependencies

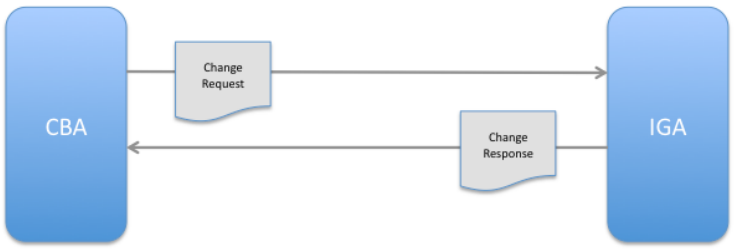
3.8.1. TBD

3.9. Assumptions

3.9.1. TBD

3.10. Process Flow

3.10.1. Process Flow Overview (figure 3)



3.10.2. The external Identity Governance Application (IGA) contacts the Cloud Based Application (CBA) and establishes a secure connection (now shown in figure3)

3.10.3. The IGA requests one of the following change request actions for a single account and passes in all required request parameters to the CBA's provisioning service point
    3.10.3.1. Create Account
    3.10.3.2. Update Account Attributes
    3.10.3.3. Assign Entitlements
    3.10.3.4. Remove Entitlements
    3.10.3.5. Enable/Disable Account
    3.10.3.6. Delete Account
3.10.4. The CBA executes the requested provisioning change and returns status information to the IGA