# Identity in the Cloud Gap Analysis Version 1.0

## Committee Note Draft 01 / Public Review Draft 01

## 29 April 2013

### Specification URIs

**This version:**

http://docs.oasis-open.org/id-cloud/IDCloud-gap/v1.0/cnprd01/IDCloud-gap-v1.0-cnprd01.doc (Authoritative)
http://docs.oasis-open.org/id-cloud/IDCloud-gap/v1.0/cnprd01/IDCloud-gap-v1.0-cnprd01.html
http://docs.oasis-open.org/id-cloud/IDCloud-gap/v1.0/cnprd01/IDCloud-gap-v1.0-cnprd01.pdf

**Previous version:**

N/A

**Latest version:**

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

**Technical Committee:**

OASIS Identity in the Cloud TC

**Chairs:**

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

**Editors:**

Gershon Janssen (gershon@qroot.com), Individual
Matt Rutkowski (mrutkows@us.ibm.com), IBM
Roger Bass (roger@traxian.com), Traxian
Dominique Nguyen (dominique.v.nguyen@bankofamerica.com), Bank of America

### Related work:

This document is related to:

- *Identity in the Cloud Use Cases Version 1.0*. Latest version. http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/IDCloud-usecases-v1.0.html.

### Abstract:

This document provides an analysis of gaps or requirements that may exist in current identity management standards. The basis for the gap analysis is the normative use cases from *Identity in the Cloud Use Cases Version 1.0*.

### 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-Gap-v1.0]**

*Identity in the Cloud Gap Analysis Version 1.0*. 29 April 2013. OASIS Committee Note Draft 01 / Public Review Draft 01. http://docs.oasis-open.org/id-cloud/IDCloud-gap/v1.0/cnprd01/IDCloud-gap-v1.0-cnprd01.html.

# 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 Identity in the Cloud TC is to:

- collect and harmonize definitions, terminologies, and vocabulary of Cloud Computing
- collect use cases to help:
    - identify gaps in existing Identity Management standards and investigate the need for profiles for achieving interoperability within current standards and
    - develop profiles of open standards for identity deployment, provisioning and management.

## 1.2 GAP analysis

The GAP analysis comprised of a detailed analysis of each Use Case from the *Identity in the Cloud Use Cases* document **[IDCloud-Usecases]**. Through this analysis the TC validated if all needs are addressed with current available standards, in such a fashion that the stated goal and outcomes are achieved.

### 1.2.1 GAP analysis process

In order to analyze each Use Case to determine how it might be implemented, what is required or find what current standards fall short or we perceive as missing, the TC followed the following step-by-step GAP analysis process:

- Based on stated goal and outcomes, consider the describe process flow, its actors, systems, and services.
- Identify relevant standards

- Drill down into the Use Case and identify big and / or rather obvious gaps in existing Identity Management and standards
- Identify commonalities and reusable elements

The outcomes of each of those steps are documented in this GAP analysis document.

### 1.2.2 GAP analysis structure outline

All outcomes of the gap analysis are documented using the following sections:

- Short description
- Covered Identity Management Categories
- Featured Cloud Deployment or Service Models
- Relevant applicable standards
- Analysis notes
- GAPs identified

## 1.3 List of relevant standards

As a result of the GAP analysis, a list of relevant applicable standards has been composed from all individual Use Cases. Chapter 2 outlines the full categorized list of current standards, versions, statuses and their maintaining organizations.

## 1.4 References

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

**[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

# 2 Relevant standards

## 2.1 Tiers of work

Standards included in this GAP analysis are standards, specifications, recommendations, notes and 'work in progress' from both SDO's as well as non-SDO's.

Applicability of the various standards work is considered in the following order:

1. OASIS SDO standards
2. Other SDOs standards
3. Specifications, recommendations and notes from SDOs and non-SDOs
4. 'Work in progress'

## 2.2 List of relevant standards

The tables below list the relevant standards.

### 2.2.1 Categorized standards and versions

**Table 1** - Column details*:*

- **Tier**: see paragraph 2.1
- **Category**: Standard category, e.g. Privacy, Authentication, Provisioning, etc.
- **Identifier**: Name and version to uniquely identify a standard. Identifiers are hyperlinked to the specification source
- **Full name**: Full name of the standard

| Tier | Category | Identifier | Full name |
|---|---|---|---|
| **1** | Authentication | DSS-1.0 | Digital Signature Services |
| **1** | Authentication | SAML-2.0 | Security Assertion Markup Language |
| **1** | Authorization | XACML-3.0 | eXtensible Access Control Markup Language |
| **1** | Fed. Identity Mgmt. | WS-Federation-1.2 | Web Services Federation Language |
| **1** | Fed. Identity Mgmt. | IMI-1.0 | Identity Metasystem Interoperability |
| **1** | Governance | ebXML CPPA-2.0 | ebXML Collaborative Partner Profile Agreement |
| **1** | Infra. Identity Mgmt. | WS-ReliableMessaging-1.2 | Web Services Reliable Messaging |
| **1** | Infra. Identity Mgmt. | WS-SecureConversation-1.4 | Web Services Secure Conversation |
| **1** | Infra. Identity | KMIP-1.1 | Key Management Interoperability Protocol |

| | | | |
|---|---|---|---|
| | Mgmt. | | Specification |
| **1** | Infra. Identity Mgmt. | WS-Transaction-1.2 | Web Services Transaction |
| **1** | Infra. Identity Mgmt. | WS-Trust-1.4 | Web Service Secure Exchange |
| **1** | Provisioning | SPML-2.0 | Service Provisioning Markup Language |
| **1** | Authentication | XMLdsig-2008 | XML Signature Syntax and Processing |
| **2** | Audit & Compliance | CADF-1.0.0 | Cloud Auditing Data Federation |
| **2** | Provisioning | CIMI-1.0.0 | Cloud Infrastructure Management Interface |
| **2** | Provisioning | CMDBf-1.0.1 | Configuration Management Database Federation |
| **2** | Virtual Machines | OVF-2.0 | Open Virtualization Format |
| **2** | Authentication | Kerberos-5 | The Kerberos Network Authentication Service |
| **2** | Authentication | RADIUS | Remote Authentication Dial In User Service |
| **2** | Authorization | OAuth-1.0 | The OAuth 1.0 Protocol |
| **2** | Authorization | OAuth-2.0 | The OAuth 2.0 Authorization Framework |
| **2** | Infra. Identity Mgmt. | IPsec | Security Architecture for the Internet Protocol |
| **2** | Infra. Identity Mgmt. | X.509-3.0 | Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile |
| **2** | Infra. Identity Mgmt. | UUID | Universally Unique IDentifier |
| **2** | Infra. Identity Mgmt. | TOTP | Time-Based One-Time Password Algorithm |
| **2** | Infra. Identity Mgmt. | HOTP | HMAC-Based One-Time Password Algorithm |
| **2** | Infra. Identity Mgmt. | LDAP-3 | Lightweight Directory Access Protocol |
| **2** | Infra. Identity Mgmt. | LDIF-1 | The LDAP Data Interchange Format |
| **2** | Assurance | ISO29115-2013 | Entity authentication assurance framework |
| **2** | Governance | ISO27018 | Code of practice for data protection controls for public cloud computing services |
| **2** | Privacy | ISO29100-2011 | Privacy framework |
| **2** | Privacy | ISO29101 | Privacy architecture framework |
| **2** | Privacy | ISO29191-2012 | Requirements for partially anonymous, partially unlinkable authentication |
| **2** | Account / Attribute Mgmt. | IGF-CARML-1.0 | Identity Governance Framework Client Attribute Requirements Markup Language |
| **2** | Account / Attribute Mgmt. | OpenID Attribute Exchange-1.0 | OpenID Attribute Exchange |
| **2** | Account / Attribute Mgmt. | OpenID Simple Registration Extension-1.0 | OpenID Simple Registration Extension |
| **2** | Authentication | OpenID Authentication-2.0 | OpenID Authentication |
| **2** | Authentication | OpenID Authentication-1.1 | OpenID Authentication |
| **2** | Authentication | OpenID Provider Authentication Policy Extension-1.0 | OpenID Provider Authentication Policy Extension |
| **2** | Infra. Identity | Backplane Protocol-2.0 | Backplane Protocol |

| | | | |
|---|---|---|---|
| | Mgmt. | | |
| 2 | Infra. Identity Mgmt. | Backplane Protocol-1.2 | Backplane Protocol |
| 2 | Infra. Identity Mgmt. | Backplane Protocol-1.1 | Backplane Protocol |
| 2 | Infra. Identity Mgmt. | Backplane Protocol-1.0 | Backplane Protocol |
| 2 | Infra. Identity Mgmt. | Account Chooser-1.0 | Account Chooser |
| 2 | Infra. Identity Mgmt. | JavaEE-6 | Java Platform Enterprise Edition |
| 2 | Infra. Identity Mgmt. | JTS-6 | Java Transaction Service |
| 2 | Infra. Identity Mgmt. | CDMI-1.0.2 | Cloud Data Management Interface |
| 2 | Infra. Identity Mgmt. | TPM-1.2 | Trusted Platform Module |
| 2 | Privacy | P3P-1.1 | Platform for Privacy Preferences |
| 3 | Assurance | EV certificates-1.4 | EV SSL Certificates |
| 3 | Provisioning | SCIM-2.0 | System for Cross-domain Identity Management |
| 3 | Provisioning | SCIM Core Schema-2.0 | System for Cross-domain Identity Management Core Schema |
| 3 | Provisioning | SCIM REST API-2.0 | System for Cross-domain Identity Management REST API |
| 3 | Provisioning | SCIM Targeting-2.0 | System for Cross-domain Identity Management Targeting |
| 3 | Privacy | PMRM-1.0 | Privacy Management Reference Model |
| 3 | Authentication | OpenID Connect-1.0 | OpenID Connect |
| 3 | Authentication | OpenID Connect Basic Client Profile-1.0 | OpenID Connect Basic Client Profile |
| 3 | Authentication | OpenID Connect Implicit Client Profile-1.0 | OpenID Connect Implicit Client Profile |
| 3 | Authentication | OpenID Connect Discovery-1.0 | OpenID Connect Discovery |
| 3 | Authentication | OpenID Connect Dynamic Client Registration-1.0 | OpenID Connect Dynamic Client Registration |
| 3 | Authentication | OpenID Connect Standard-1.0 | OpenID Connect Standard |
| 3 | Authentication | OpenID Connect Messages-1.0 | OpenID Connect Messages |
| 3 | Authentication | OpenID Connect Session Management-1.0 | OpenID Connect Session Management |
| 3 | Authorization | OpenID Connect OAuth 2.0 Multiple Response Type Encoding Practices-1.0 | OpenID Connect OAuth 2.0 Multiple Response Type Encoding Practices |
| 3 | Lifecycle | OSLC | Open Services for Lifecycle Collaboration |
| 3 | Lifecycle | OSLC Core-3.0 | Open Services for Lifecycle Collaboration - Common and Core |
| 3 | Lifecycle | OSLC Core-2.0 | Open Services for Lifecycle Collaboration - Commen and Core |
| 3 | Lifecycle | OSLC Configuration Management-1.0 | Open Services for Lifecycle Collaboration - Configuration Management |
| 3 | Provisioning | SCIM-1.1 | System for Cross-domain Identity Management |

| | | | |
|---|---|---|---|
| **3** | Provisioning | SCIM Core Schema-1.1 | System for Cross-domain Identity Management Core Schema |
| **3** | Provisioning | SCIM REST API-1.1 | System for Cross-domain Identity Management REST API |
| **3** | Privacy | P3P-1.0 | Platform for Privacy Preferences |
| **4** | Audit & Compliance | CloudAudit-1.0 | CloudAudit - Automated Audit, Assertion, Assessment, and Assurance API |
| **4** | Authentication | JWS-0.8 | JSON Web Signature |
| **4** | Authentication | JWT-0.6 | JSON Web Token |
| **4** | Audit & Compliance | ISO27017-1.0.0 | Guidelines on information security controls for the use of cloud computing services |
| **4** | Authorization | UMA-0.7 | User-Managed Access Profile of OAuth 2.0 |
| **4** | Assurance | Trust Elevation | Electronic Identity Credential Trust Elevation Methods |
| **4** | Lifecycle | TOSCA-1.0 | Topology and Orchestration Specification for Cloud Applications |

### 2.2.2 Standards, versions, status and managing Organization

**Table 2** - Column details*:*

- **Identifier**: Name and version to uniquely identify a standard. Identifiers are hyperlinked to the specification source

- **Version**: Version of the standard, specification or recommendation

- **Organization**: Organization who maintains and publishes the standard. Organization names are hyperlinked to their respective Internet web pages.

- **Status**: State of the standard, e.g. Standard, Draft Specification, Note.

| Identifier | Version | Organization | | Status |
|---|---|---|---|---|
| **DSS-1.0** | 1.0 | OASIS | Organization for the Advancement of Structured Information Standards | Standard |
| **SAML-2.0** | 2.0 | OASIS | Organization for the Advancement of Structured Information Standards | Standard |
| **XACML-3.0** | 3.0 | OASIS | Organization for the Advancement of Structured Information Standards | Standard |
| **WS-Federation-1.2** | 1.2 | OASIS | Organization for the Advancement of Structured Information Standards | Standard |
| **IMI-1.0** | 1.0 | OASIS | Organization for the Advancement of Structured Information Standards | |
| **ebXML CPPA-2.0** | 2.0 | OASIS | Organization for the Advancement of Structured Information Standards | Standard |
| **WS-ReliableMessaging-1.2** | 1.2 | OASIS | Organization for the Advancement of Structured Information Standards | Standard |
| **WS-SecureConversation-1.4** | 1.4 | OASIS | Organization for the | Standard |

| | | | | |
|---|---|---|---|---|
| | | | Advancement of Structured Information Standards | |
| **KMIP-1.1** | 1.1 | OASIS | Organization for the Advancement of Structured Information Standards | Standard |
| **WS-Transaction-1.2** | 1.2 | OASIS | Organization for the Advancement of Structured Information Standards | Standard |
| **WS-Trust-1.4** | 1.4 | OASIS | Organization for the Advancement of Structured Information Standards | Standard |
| **SPML-2.0** | 2.0 | OASIS | Organization for the Advancement of Structured Information Standards | Standard |
| **XMLdsig-2008** | 2008 | W3C | The World Wide Web Consortium | Recommendation |
| **CADF-1.0.0** | 1.0.0 | DMTF | Distributed Management Task Force | Draft Specification |
| **CIMI-1.0.0** | 1.0.0 | DMTF | Distributed Management Task Force | Specification |
| **CMDBf-1.0.1** | 1.0.1 | DMTF | Distributed Management Task Force | Specification |
| **OVF-2.0** | 2.0 | DMTF | Distributed Management Task Force | Standard |
| **Kerberos-5** | 5 | IETF | Internet Engineering Task Force | Standard |
| **RADIUS** | | IETF | Internet Engineering Task Force | Standard |
| **OAuth-1.0** | 1.0 | IETF | Internet Engineering Task Force | Standard |
| **OAuth-2.0** | 2.0 | IETF | Internet Engineering Task Force | Standard |
| **IPsec** | | IETF | Internet Engineering Task Force | Standard |
| **X.509-3.0** | 3.0 | IETF | Internet Engineering Task Force | Standard |
| **UUID** | | IETF | Internet Engineering Task Force | Standard |
| **TOTP** | | IETF | Internet Engineering Task Force | Standard |
| **HOTP** | | IETF | Internet Engineering Task Force | Standard |
| **LDAP-3** | 3 | IETF | Internet Engineering Task Force | Standard |
| **LDIF-1** | 1 | IETF | Internet Engineering Task Force | Standard |
| **ISO29115-2013** | 2013 | ISO | International Organization for Standardization | Standard |
| **ISO27018** | | ISO | International Organization for Standardization | Work in progress |
| **ISO29100-2011** | 2011 | ISO | International Organization for Standardization | Standard |
| **ISO29101** | | ISO | International Organization for Standardization | Work in progress |
| **ISO29191-2012** | 2012 | ISO | International Organization for Standardization | Standard |

| | | | | |
|---|---|---|---|---|
| **IGF-CARML-1.0** | 1.0 | Liberty Alliance | Liberty Alliance | Specification |
| **OpenID Attribute Exchange-1.0** | 1.0 | OIDF | OpenID Foundation | Specification |
| **OpenID Simple Registration Extension-1.0** | 1.0 | OIDF | OpenID Foundation | Specification |
| **OpenID Authentication-2.0** | 2.0 | OIDF | OpenID Foundation | Specification |
| **OpenID Authentication-1.1** | 1.1 | OIDF | OpenID Foundation | Specification |
| **OpenID Provider Authentication Policy Extension-1.0** | 1.0 | OIDF | OpenID Foundation | Specification |
| **Backplane Protocol-2.0** | 2.0 | OIDF | OpenID Foundation | Draft Specification |
| **Backplane Protocol-1.2** | 1.2 | OIDF | OpenID Foundation | Specification |
| **Backplane Protocol-1.1** | 1.1 | OIDF | OpenID Foundation | Specification |
| **Backplane Protocol-1.0** | 1.0 | OIDF | OpenID Foundation | Specification |
| **Account Chooser-1.0** | 1.0 | OIDF | OpenID Foundation | Specification |
| **JavaEE-6** | 6 | Oracle | Oracle Corporation | Specification |
| **JTS-6** | 6 | Oracle | Oracle Corporation | Specification |
| **CDMI-1.0.2** | 1.0.2 | SNIA | The Storage Networking Industry Association | Standard |
| **TPM-1.2** | 1.2 | TCG | Trusted Computing Group | Standard |
| **P3P-1.1** | 1.1 | W3C | The World Wide Web Consortium | Draft Specification |
| **EV certificates-1.4** | 1.4 | CABForum | CA/Browser Forum | Specification |
| **SCIM-2.0** | 2.0 | IETF | Internet Engineering Task Force | Draft Specification |
| **SCIM Core Schema-2.0** | 2.0 | IETF | Internet Engineering Task Force | Draft Specification |
| **SCIM REST API-2.0** | 2.0 | IETF | Internet Engineering Task Force | Draft Specification |
| **SCIM Targeting-2.0** | 2.0 | IETF | Internet Engineering Task Force | Draft Specification |
| **PMRM-1.0** | 1.0 | OASIS | Organization for the Advancement of Structured Information Standards | Draft Specification |
| **OpenID Connect-1.0** | 1.0 | OIDF | OpenID Foundation | Draft Specification |
| **OpenID Connect Basic Client Profile-1.0** | 1.0 | OIDF | OpenID Foundation | Draft Specification |
| **OpenID Connect Implicit Client Profile-1.0** | 1.0 | OIDF | OpenID Foundation | Draft Specification |
| **OpenID Connect Discovery-1.0** | 1.0 | OIDF | OpenID Foundation | Draft Specification |
| **OpenID Connect Dynamic Client Registration-1.0** | 1.0 | OIDF | OpenID Foundation | Draft Specification |
| **OpenID Connect Standard-1.0** | 1.0 | OIDF | OpenID Foundation | Draft Specification |
| **OpenID Connect Messages-1.0** | 1.0 | OIDF | OpenID Foundation | Draft Specification |
| **OpenID Connect Session Management-1.0** | 1.0 | OIDF | OpenID Foundation | Draft Specification |
| **OpenID Connect OAuth 2.0** | 1.0 | OIDF | OpenID Foundation | Draft Specification |

| | | | | |
|---|---|---|---|---|
| **Multiple Response Type Encoding Practices-1.0** | | | | |
| **OSLC** | | OSLC | Open Services for Lifecycle Collaboration | |
| **OSLC Core-3.0** | 3.0 | OSLC | Open Services for Lifecycle Collaboration | Draft Specification |
| **OSLC Core-2.0** | 2.0 | OSLC | Open Services for Lifecycle Collaboration | Specification |
| **OSLC Configuration Management-1.0** | 1.0 | OSLC | Open Services for Lifecycle Collaboration | Draft Specification |
| **SCIM-1.1** | 1.1 | OWF | Open Web Foundation | Specification |
| **SCIM Core Schema-1.1** | 1.1 | OWF | Open Web Foundation | Specification |
| **SCIM REST API-1.1** | 1.1 | OWF | Open Web Foundation | Specification |
| **P3P-1.0** | 1.0 | W3C | The World Wide Web Consortium | Specification |
| **CloudAudit-1.0** | 1.0 | CSA | Cloud Security Alliance | Draft Specification |
| **JWS-0.8** | 0.8 | IETF | Internet Engineering Task Force | Draft |
| **JWT-0.6** | 0.6 | IETF | Internet Engineering Task Force | Draft |
| **ISO27017-1.0.0** | 1.0.0 | ISO | International Organization for Standardization | Work in progress |
| **UMA-0.7** | 0.7 | Kantara Initiative | Kantara Initiative | Draft Specification |
| **Trust Elevation** | | OASIS | Organization for the Advancement of Structured Information Standards | Work in progress |
| **TOSCA-1.0** | 1.0 | OASIS | Organization for the Advancement of Structured Information Standards | Specification |

# 3 Gap Analysis per Use Case

## 3.1 Use Case 1: Application and Virtualization Security in the Cloud

### 3.1.1 Short description

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.

### 3.1.2 Covered Identity Management Categories

| **Infra. Identity Est.** | **Identity Mgmt.** | | | **Authentication** | | | **Authorization** | **Account / Attribute Mgmt.** | | **Security Tokens** | **Governance** | **Audit & Compliance** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ***Gen.*** | ***IIM*** | ***FIM*** | ***Gen.*** | ***SSO*** | ***Multi-Factor*** | | ***Gen.*** | ***Provisioning*** | | | |
| | P | P | S | | | | | S | | | | |

### 3.1.3 Featured Cloud Deployment or Service Models

| **Featured Cloud Deployment Models** | | | | | **Featured Cloud Service Models** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| | X | X | | | | | X | X | |

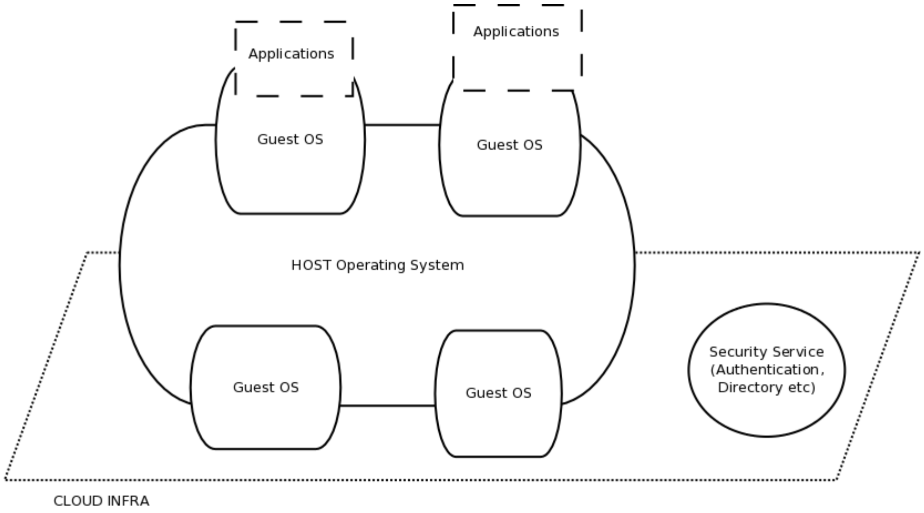
### 3.1.4 Relevant applicable standards

- Account / Attribute Mgmt.; OpenID Attribute Exchange-1.0
- Account / Attribute Mgmt.; OpenID Simple Registration Extension-1.0
- Authentication; SAML-2.0
- Authentication; RADIUS
- Authentication; OpenID Authentication-2.0
- Authentication; OpenID Authentication-1.1
- Authorization; OAuth-2.0
- Infra. Identity Mgmt.; WS-Trust-1.4
- Infra. Identity Mgmt.; IPsec
- Infra. Identity Mgmt.; LDAP-3
- Provisioning; SPML-2.0
- Provisioning; SCIM Core Schema-2.0
- Provisioning; SCIM REST API-2.0
- Provisioning; SCIM Targeting-2.0

- Virtual Machines; OVF-2.0

### 3.1.5 Analysis notes

- The diagram is a pictorial representation of the use case



- The Cloud Provider's Identity Mgmt. System is able to handle identity management for multiple tenants on various infrastructure levels.
- Multiple administrator roles exist: for servers, host OS, virtual machines, guest OS and applications.
- Each administrative role has its own scope: what it can do, or should not be able to do. E.g. a Virtual Machine administrator can provision and decommission / destroy Virtual Machines, but cannot access the actual runtime.
- A user becomes an administrative user (in any role) by group membership(s) or special attribute(s) being set. Typically attributes map to LDAP / X.500 group memberships.
- Authentication for administrative users requires being strong and / or multi-factor.
- The identity store plays an important role in this use case. Administrative users may be required to exist in different stores, e.g. at the server level in password files or in network based directory services such as yellow pages.
- In an ideal world one could create this by using one single directory service.
- How to handle ownership of identities in multi-tenant setups?
- There is a requirement for the uniqueness of identities and devices. Virtual machines, appliances, switches, etc. should be uniquely identified.

### 3.1.6 GAPs identified

- **No standards for attribute management.** There are no particular standards for attribute management.
    - Attributes and LDAP / X.500 group memberships are not universal; there is a need for wider standardization on attributes and groups, e.g. for administrative users.
    - Such standardization should also allow for specific groups for Subscribers and Providers, so they are not intermingled.
- **No unique identifier for virtual machines.** There is a requirement for the uniqueness of identities and devices. Virtual machines, appliances, switches, etc. should be uniquely identified.
    - Most standards that include IDs often don't make recommendations for uniqueness in virtual machines, appliances, software, etc.
    - This would allow meeting audit requirements.
- **No unambiguous definition of Virtual Machine.** The definition of a Virtual Machine is not unambiguous.

## 3.2 Use Case 2: Identity Provisioning

### 3.2.1 Short description

Feature the need support and manage customer policies for identity decommissioning including transitioning of affected resources to new identities.

### 3.2.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.2.3 Featured Cloud Deployment or Service Models

| Featured Cloud Deployment Models | | | | | Featured Cloud Service Models | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.2.4 Relevant applicable standards

- Provisioning; CIMI-1.0.0
- Infra. Identity Mgmt.; UUID
- Provisioning; SPML-2.0
- Provisioning; SCIM Core Schema-2.0
- Provisioning; SCIM-2.0
- Provisioning; SCIM REST API-2.0
- Provisioning; SCIM Targeting-2.0
- Lifecycle; OSLC Core-3.0
- Lifecycle; OSLC Core-2.0
- Lifecycle; OSLC Configuration Management-1.0

### 3.2.5 Analysis notes

- Provisions and policies for life cycle management.

### 3.2.6 GAPs identified

- **No standard policies for life cycle management.**

- **No standards based provisioning and disposal of virtual entities.**
    - CRUD of Virtual Entities.
    - Commissioning / decommissioning of cloud resources, including their attributes.
- **No transitioning of owned resources when an identity is decommissioned.** Transitioning of resources (including their attributes) to a different identity when a particular identity is decommissioned.
    - Preserving identities' roles and attributes may be done through mapping.

## 3.3 Use Case 3: Identity Audit

### 3.3.1 Short description

Feature the importance of auditing/logging of sensitive operations performed by users and administrators in the cloud.

### 3.3.2 Covered Identity Management Categories

| **Infra. Identity Est.** | **Identity Mgmt.** | | | **Authentication** | | | **Authorization** | **Account / Attribute Mgmt.** | | **Security Tokens** | **Governance** | **Audit & Compliance** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ***Gen.*** | ***IIM*** | ***FIM*** | ***Gen.*** | ***SSO*** | ***Multi-Factor*** | | ***Gen.*** | ***Provisioning*** | | | |
| | | | | | | | | | | | | P |

### 3.3.3 Featured Cloud Deployment or Service Models

| **Featured Cloud Deployment Models** | | | | | **Featured Cloud Service Models** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | X | | | | |

### 3.3.4 Relevant applicable standards

- Audit & Compliance; CloudAudit-1.0
- Audit & Compliance; ISO27017-1.0.0

### 3.3.5 Analysis notes

- When speaking about auditing, we need to be clear on what type of auditing, e.g. technical, business, policy, etc.

- Policy auditing: notion of trying to show there is a relation between policies.

- Need to have better auditing (introspection) standards that can be automated to show security compliance (with identities) in virtual cloud environments that include the three IaaS aspects of cloud (i.e. compute in terms of hypervisor/virtual machine auditing, storage/managed storage like DB access, and network to verify network routes are secured) and that the multi-tenant aspects of these resources are considered

- An area for auditing is to provide proof of isolation in multi-tenant environments

- NIST Mitre (CEE) standards were an attempt for traditional platforms, but they do not translate well to cloud
- Audit trails of various different systems (logs, etc.)
- Things that need to be tracked are specified in compliance rules
- Highlighted by cloud use: what needs to be logged to do effective auditing?
- Try to maintain key aspects of a transaction (e.g. identity, identity of resources involved, who grants authority to execute a transaction ); not specifically the format, but the identifiers
- new types of policies required for auditing due to different ownership requirements → may imply new data elements required for audit

### 3.3.6 Possible GAPs identified

The following possible GAPs have been identified:

- No real standards on auditing for the cloud space; applicable to all auditing elements in use cases so far.
- Uniqueness of identities (as made in use case 1)
  - Also: who is providing identities
  - Who authorized
  - Consumer and provider identities
- No audit standard for IDM systems
- No common audit trail standard to support the audit capabilities

## 3.4 Use Case 4: Identity Configuration

### 3.4.1 Short description

Feature the need for portable standards to configure identities in cloud applications and infrastructure (virtual machines, servers etc).

### 3.4.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.4.3 Featured Cloud Deployment or Service Models

| Featured Cloud Deployment Models | | | | | Featured Cloud Service Models | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.4.4 Relevant applicable standards

- Authentication; SAML-2.0
- Infra. Identity Mgmt.; LDIF-1
- Infra. Identity Mgmt.; LDAP-3
- Virtual Machines; OVF-2.0
- Lifecycle; TOSCA-1.0

### 3.4.5 Analysis notes

- LDIFF can be used as a means for migration of identities from LDAP directories

- There is a SAML construct for sending identity information (SAML assertions about an identity from a trusted third party will result in creation the identity). Namespaces are present in SAML attributes.

- OVF can help migrate a virtual machine between two cloud providers, though metadata for migrating identities and attributes are not standardized.

- These are standards that contain types of data that are described in use case 1, and might need to look at the gaps in this use case

### 3.4.6 Possible GAPs identified

The following possible GAPs have been identified:

- Two levels to describe: at a resource level and at a service level. E.g. account level identity and a specific identity / assertion for resource or application
- See use case 1
- Federation of data described in use case 1 (or others) between cloud boundaries.

## 3.5 Use Case 5: Middleware Container in a Public Cloud

### 3.5.1 Short description

Show how cloud identities need to be administered and accounted for in order to manage middleware containers and their applications.

### 3.5.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.5.3 Featured Cloud Deployment or Service Models

| Featured Cloud Deployment Models | | | | | Featured Cloud Service Models | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *None* | *Private* | *Public* | *Community* | *Hybrid* | *None* | *SaaS* | *PaaS* | *IaaS* | *Other* |
| X | | | | | | X | | | |

### 3.5.4 Relevant applicable standards

- Account / Attribute Mgmt.; OpenID Attribute Exchange-1.0
- Account / Attribute Mgmt.; OpenID Simple Registration Extension-1.0
- Authentication; SAML-2.0
- Authentication; OpenID Authentication-2.0
- Authentication; OpenID Authentication-1.1
- Authentication; OpenID Provider Authentication Policy Extension-1.0
- Infra. Identity Mgmt.; JavaEE-6
- Virtual Machines; OVF-2.0
- Lifecycle; TOSCA-1.0

### 3.5.5 Analysis notes

- About other pieces of middleware that may introduce new types of system identities, for tracking across cloud infrastructures

- For application deployment, what types of middleware containers and services may be permitted to host the application or data.

### 3.5.6 Possible GAPs identified

- Manage against policies
- Correct mapping of roles and relation to identities
- Virtualized instances id propagation needs to be considered in scaling applications, e.g. database instance id

## 3.6 Use Case 6: Federated SSO and Attribute Sharing

### 3.6.1 Short description

Feature the need for Federated Single Sign-On (F-SSO) across multiple cloud environments.

### 3.6.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.6.3 Featured Cloud Deployment or Service Models

| **Featured Cloud Deployment Models** | | | | | **Featured Cloud Service Models** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.6.4 Relevant applicable standards

- Account / Attribute Mgmt.; OpenID Attribute Exchange-1.0
- Authorization; XACML-3.0
- Fed. Identity Mgmt.; IMI-1.0
- Account / Attribute Mgmt.; OpenID Simple Registration Extension-1.0
- Authentication; SAML-2.0
- Authentication; OpenID Authentication-2.0
- Authentication; OpenID Authentication-1.1
- Authorization; OAuth-2.0
- Infra. Identity Mgmt.; WS-Trust-1.4
- Assurance; ISO29115-2013
- Authentication; OpenID Provider Authentication Policy Extension-1.0
- Authentication; OpenID Connect-1.0
- Authentication; OpenID Connect Basic Client Profile-1.0
- Authentication; OpenID Connect Implicit Client Profile-1.0
- Authentication; OpenID Connect Discovery-1.0
- Authentication; OpenID Connect Dynamic Client Registration-1.0
- Authentication; OpenID Connect Standard-1.0
- Authentication; OpenID Connect Messages-1.0

- Authentication; OpenID Connect Session Management-1.0
- Authorization; OpenID Connect OAuth 2.0 Multiple Response Type Encoding Practices-1.0
- Authorization; UMA-0.7

### 3.6.5 Analysis notes

- Inter-cloud back-to-back operations are required to support and / or allow the exchange of attributes in order to establish the desired trust
- WS-Trust seems applicable for setting up token claims, even with various intermediaries / brokers
- The exchange of tokens if possible but identity mapping is not possible. Once one gets a token, the attributes are not available.
- Native attribute sharing / exchange not possible, as the ontology is not the same (definitions are not the same / harmonized)
- Token might be related to an identity, or be an attribute by itself
- Different parties who might own the attributes (ownership of attributes); different attributes coming from various sources; might want to add attributes to it; level of trust between authorities who provide attributes (level of trust behind provider of attribute)
- Use and availability of attributes;

### 3.6.6 Possible GAPs identified

The following possible GAPs have been identified:

- Relates to use case 4, with respect to attributes
- Standardized mechanisms for token exchange and desired subsequent attribute sharing are absent
- Attributes of attributes, e.g. trust put in a given attribute. E.g. Authority that is the source /provider of the attribute which is the guarantor of it. Information about the provenance of the attributes, e.g. trust levels, source, information about the authority, etc.

## 3.7 Use Case 7: Identity Silos in the Cloud

### 3.7.1 Short description

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

### 3.7.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.7.3 Featured Cloud Deployment or Service Models

| Featured Cloud Deployment Models | | | | | Featured Cloud Service Models | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *None* | *Private* | *Public* | *Community* | *Hybrid* | *None* | *SaaS* | *PaaS* | *IaaS* | *Other* |
| X | | | | | | X | | | |

### 3.7.4 Relevant applicable standards

- Fed. Identity Mgmt.; WS-Federation-1.2
- Authentication; SAML-2.0
- Infra. Identity Mgmt.; WS-Trust-1.4
- Infra. Identity Mgmt.; LDAP-3
- Authentication; OpenID Connect-1.0
- Authentication; OpenID Connect Basic Client Profile-1.0
- Authentication; OpenID Connect Implicit Client Profile-1.0
- Authentication; OpenID Connect Discovery-1.0
- Authentication; OpenID Connect Dynamic Client Registration-1.0
- Authentication; OpenID Connect Standard-1.0
- Authentication; OpenID Connect Messages-1.0
- Authentication; OpenID Connect Session Management-1.0
- Authorization; OpenID Connect OAuth 2.0 Multiple Response Type Encoding Practices-1.0

### 3.7.5 Analysis notes

- Basically any standard that span multiple directory services and can get a consolidated view are applicable.
- The Cloud Identity Management System should have the ability to pull information from multiple directory services, irrespective of where it is located
- Known federation techniques WS-Trust, WS-Federation, SAML, OpenID Connect for targeting different scenarios (OpenID Connect maybe not for enterprise solutions, but for 'lower risk' or 'lower levels of assurance' scenarios).
- Refer to SAML attributes statements and WS-Trust claims

### 3.7.6 Possible GAPs identified

- Map or transform attributes between different (cloud) domains. There could be an agreement + rules for mapping. Also show / retain / provide an audit trail that mapping has been performed.
- If identity information has been modified or transformed, it’s something that needs to be audited.
- Within an industry (backing, finance, health care) define profiles for attributes; between industry or overall is difficult or impossible (it applying to all processes);
- Should be possible to define standard roles and related attributes from a provider perspective, though the cloud architectures still under design and changing
- Naming of attributes of important: e.g. calling someone a ‘manager’ might be meaningful, relevant, and important.

## 3.8 Use Case 8: Identity Privacy in a Shared Cloud Environment

### 3.8.1 Short description

Show the need for controls to exist to maintain privacy of identities while operating in a cloud if desired.

### 3.8.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.8.3 Featured Cloud Deployment or Service Models

| Featured Cloud Deployment Models | | | | | Featured Cloud Service Models | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *None* | *Private* | *Public* | *Community* | *Hybrid* | *None* | *SaaS* | *PaaS* | *IaaS* | *Other* |
| X | | | | | | X | | | |

### 3.8.4 Relevant applicable standards

- Authorization; XACML-3.0
- Governance; ISO27018
- Privacy; ISO29100-2011
- Privacy; ISO29101
- Privacy; ISO29191-2012
- Privacy; P3P-1.1
- Privacy; PMRM-1.0

### 3.8.5 Analysis notes

- Standards are with respect to preferences on privacy controls such as attributes of the identity. Preferences such as 'what I like' and attributes such as 'age and height' are not applicable.

- There are a number of ISO standards (being developed) that are intended to address privacy controls.

- These include technology aspects for expressing policy, but also the procedural aspects and data protection in a cloud context, with respect to sensitive information in the cloud

### 3.8.6 Possible GAPs identified

- Access control to a particular attribute or purpose of use for an attribute; no namespace for this now.
- Declare policies for use of individual attribues.
- In health-care (xspa tc), due to purpose of use (emergency) the access policy can be overridden.

## 3.9 Use Case 9: Cloud Signature Services

### 3.9.1 Short description

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.

### 3.9.2 Covered Identity Management Categories

| **Infra. Identity Est.** | **Identity Mgmt.** | | | **Authentication** | | | **Authorization** | **Account / Attribute Mgmt.** | | **Security Tokens** | **Governance** | **Audit & Compliance** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ***Gen.*** | ***IIM*** | ***FIM*** | ***Gen.*** | ***SSO*** | ***Multi-Factor*** | | ***Gen.*** | ***Provisioning*** | | | |
| | P | | | | | | | P | | | | |

### 3.9.3 Featured Cloud Deployment or Service Models

| **Featured Cloud Deployment Models** | | | | | **Featured Cloud Service Models** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.9.4 Relevant applicable standards

- Authentication; DSS-1.0
- Authentication; XMLdsig-2008
- Authentication; JWS-0.8
- Authentication; JWT-0.6

### 3.9.5 Analysis notes

- Focus of the use case is signatures.
- Use case about a service in the cloud the provide signatures / sign documents.
- Basic functionalities of signing and verifying are specified, as are specialized profiles.
- JWS may be relevant to cloud if the API uses JSON based transport.
- Office365/google docs: no access to local resources to do signing.
- To sign: method + input (as keys)

- See background DSS TC; see how it works, put in a cloud context and generalize for other documents
- Declare operations / security services available to cloud providers which can support the signing, exchange of required keys, etc.

### 3.9.6 Possible GAPs identified

- Perhaps a specialized profile is needed.

## 3.10 Use Case 10: Cloud Tenant Administration

### 3.10.1 Short description

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).

### 3.10.2 Covered Identity Management Categories

| **Infra. Identity Est.** | **Identity Mgmt.** | | | **Authentication** | | | **Authorization** | **Account / Attribute Mgmt.** | | **Security Tokens** | **Governance** | **Audit & Compliance** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ***Gen.*** | ***IIM*** | ***FIM*** | ***Gen.*** | ***SSO*** | ***Multi-Factor*** | | ***Gen.*** | ***Provisioning*** | | | |
| | P | | | | | | | P | | | | |

### 3.10.3 Featured Cloud Deployment or Service Models

| **Featured Cloud Deployment Models** | | | | | **Featured Cloud Service Models** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.10.4 Relevant applicable standards

- Account / Attribute Mgmt.; OpenID Attribute Exchange-1.0
- Account / Attribute Mgmt.; OpenID Simple Registration Extension-1.0
- Authentication; SAML-2.0
- Audit & Compliance; CADF-1.0.0
- Authentication; OpenID Authentication-2.0
- Authentication; OpenID Provider Authentication Policy Extension-1.0

### 3.10.5 Analysis notes

- Level of Assurance is relevant within the context of the use case.
- Relevant here is mapping of identities to cloud resources. Relationship can be handles/owns.
- Relevant here is storage of information that may have compliance requirements.

- Priviledged user actions – tenant operations should be considered as such; put audit control on them
- Many types of admins at different levels (represent unique roles in the systems) and should be treated privileged users and considered separate and independent of each other. Importance of doing this is for auditing purposes.
- In an environment exposing admin functions / create a new level of privileged actions, integrate with cloud provider audit functions.
- Domain level privileges for services and roles for them are separate; admin privileges cannot assumed to be translated between domains.
- This use case is applicable to any number of domains where admin actions exists.
    - Reason why we cannot have a generalized set of roles

### 3.10.6 Possible GAPs identified

- Possible GAPs depend on the cloud provider architecture being used. In this example 3 levels of admins, but could design as e.g. 10 levels of admins.
- Wherever std being developed for cloud architectures, the analysis in this use case should be considered in them

## 3.11 Use Case 11: Enterprise to Cloud SSO

### 3.11.1 Short description

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.

### 3.11.2 Covered Identity Management Categories

| **Infra. Identity Est.** | **Identity Mgmt.** | | | **Authentication** | | | **Authorization** | **Account / Attribute Mgmt.** | | **Security Tokens** | **Governance** | **Audit & Compliance** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ***Gen.*** | ***IIM*** | ***FIM*** | ***Gen.*** | ***SSO*** | ***Multi-Factor*** | | ***Gen.*** | ***Provisioning*** | | | |
| | P | | | | | | | P | | | | |

### 3.11.3 Featured Cloud Deployment or Service Models

| **Featured Cloud Deployment Models** | | | | | **Featured Cloud Service Models** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.11.4 Relevant applicable standards

- Account / Attribute Mgmt.; OpenID Attribute Exchange-1.0
- Account / Attribute Mgmt.; OpenID Simple Registration Extension-1.0
- Authentication; SAML-2.0
- Authentication; OpenID Authentication-2.0
- Provisioning; SPML-2.0
- Provisioning; SCIM Core Schema-2.0
- Authentication; OpenID Provider Authentication Policy Extension-1.0
- Provisioning; SCIM-2.0

- Provisioning; SCIM REST API-2.0
- Provisioning; SCIM Targeting-2.0
- Authentication; OpenID Connect-1.0
- Authentication; OpenID Connect Basic Client Profile-1.0
- Authentication; OpenID Connect Implicit Client Profile-1.0
- Authentication; OpenID Connect Discovery-1.0
- Authentication; OpenID Connect Dynamic Client Registration-1.0
- Authentication; OpenID Connect Standard-1.0
- Authentication; OpenID Connect Messages-1.0
- Authentication; OpenID Connect Session Management-1.0
- Authorization; OpenID Connect OAuth 2.0 Multiple Response Type Encoding Practices-1.0

### 3.11.5 Analysis notes

- Provisioning standards are relevant as they are needed for creation of identities and synchronization of identities between enterprises and pubic cloud providers.

- ISO SC38/WG1 and ISO SC38/WG3 activities might be relevant for this use case.

- Application should be able to, when receiving a SSO token, reverify if the token can be sufficiently trusted and / or learn more about the token before using it

### 3.11.6 Possible GAPs identified

- Require to known attributes about the token, to determine in a standards way if the token is usable for our service. If attributes indicate it is not appropriate for our use, we should be able to go to a service to step-up to a valid token with more attributes / more information about the attributes /correct insurance trust levels about the attributes.

- Elements like: how long ago have these attributes been created; where did they come from?

- Indication of time, step-up to add more attributes.

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

### 3.12.1 Short description

A user (or cloud consumer) is able to access multiple SaaS applications using a single identity.

### 3.12.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.12.3 Featured Cloud Deployment or Service Models

| Featured Cloud Deployment Models | | | | | Featured Cloud Service Models | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *None* | *Private* | *Public* | *Community* | *Hybrid* | *None* | *SaaS* | *PaaS* | *IaaS* | *Other* |
| X | | | | | | X | | | |

### 3.12.4 Relevant applicable standards

- Account / Attribute Mgmt.; OpenID Attribute Exchange-1.0
- Fed. Identity Mgmt.; WS-Federation-1.2
- Fed. Identity Mgmt.; IMI-1.0
- Account / Attribute Mgmt.; OpenID Simple Registration Extension-1.0
- Authentication; SAML-2.0
- Authentication; OpenID Authentication-2.0
- Authentication; OpenID Authentication-1.1
- Authorization; OAuth-2.0
- Provisioning; SPML-2.0
- Provisioning; SCIM Core Schema-2.0
- Authentication; OpenID Provider Authentication Policy Extension-1.0
- Provisioning; SCIM-2.0
- Provisioning; SCIM REST API-2.0
- Provisioning; SCIM Targeting-2.0

### 3.12.5 Analysis notes

- Attribute management is relevant for this use case.
- Trust frameworks are relevant for this use case.
- Service and preferred IdP? List of IdPs? How to interact with the IdP (e.g. protocol), etc.
- Completely remove all identity from the cloud provider.

### 3.12.6 Possible GAPs identified

- Configuration and association with IdP is not standardized. No standard way to set this up.
- External IdPs need to consider all other GAPs that have been identified  other use cases

## 3.13 Use Case 13: Transaction Validation and Signing in the Cloud

### 3.13.1 Short description

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

### 3.13.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.13.3 Featured Cloud Deployment or Service Models

| Featured Cloud Deployment Models | | | | | Featured Cloud Service Models | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *None* | *Private* | *Public* | *Community* | *Hybrid* | *None* | *SaaS* | *PaaS* | *IaaS* | *Other* |
| X | | | | | | X | | | |

### 3.13.4 Relevant applicable standards

- Infra. Identity Mgmt.; WS-Transaction-1.2
- Authentication; SAML-2.0
- Infra. Identity Mgmt.; X.509-3.0
- Infra. Identity Mgmt.; JTS-6

### 3.13.5 Analysis notes

- Smart card standards seem relevant to this use case, though it a large domain, e.g. FIPS 140-2, ANSI X9 series financial standards

- Biometric standards seem relevant to this use case. Groups with activities within this space are INCITS M1, ISO/IEC JTC1 SC37, ISO/IEC JTC1 SC27.

- PKI standards

- Authentication used to validate the signer (e.g. SAML auth_context_class)

- Value in communicating the determine if enough

### 3.13.6 Possible GAPs identified

## 3.14 Use Case 14: Enterprise Purchasing from a Public Cloud

### 3.14.1 Short description

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” architecture.

### 3.14.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.14.3 Featured Cloud Deployment or Service Models

| Featured Cloud Deployment Models | | | | | Featured Cloud Service Models | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *None* | *Private* | *Public* | *Community* | *Hybrid* | *None* | *SaaS* | *PaaS* | *IaaS* | *Other* |
| X | | | | | | X | | | |

### 3.14.4 Relevant applicable standards

- Account / Attribute Mgmt.; OpenID Attribute Exchange-1.0
- Fed. Identity Mgmt.; WS-Federation-1.2
- Account / Attribute Mgmt.; OpenID Simple Registration Extension-1.0
- Authentication; SAML-2.0
- Authentication; OpenID Authentication-2.0
- Authorization; OAuth-2.0
- Infra. Identity Mgmt.; X.509-3.0
- Infra. Identity Mgmt.; WS-Trust-1.4
- Provisioning; SPML-2.0
- Authentication; OpenID Provider Authentication Policy Extension-1.0

### 3.14.5 Analysis notes

- Level of Assurance is relevant within the context of the use case.

- Trust frameworks are relevant for this use case.

- PKI standards are relevant for this use case

### 3.14.6 Possible GAPs identified

## 3.15 Use Case 15: Access to Enterprise's Workforce Applications Hosted in Cloud

### 3.15.1 Short description

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.

### 3.15.2 Covered Identity Management Categories

| **Infra. Identity Est.** | **Identity Mgmt.** | | | **Authentication** | | | **Authorization** | **Account / Attribute Mgmt.** | | **Security Tokens** | **Governance** | **Audit & Compliance** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ***Gen.*** | ***IIM*** | ***FIM*** | ***Gen.*** | ***SSO*** | ***Multi-Factor*** | | ***Gen.*** | ***Provisioning*** | | | |
| | P | | | | | | | P | | | | |

### 3.15.3 Featured Cloud Deployment or Service Models

| **Featured Cloud Deployment Models** | | | | | **Featured Cloud Service Models** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.15.4 Relevant applicable standards

- Account / Attribute Mgmt.; OpenID Attribute Exchange-1.0
- Authorization; XACML-3.0
- Fed. Identity Mgmt.; WS-Federation-1.2
- Account / Attribute Mgmt.; OpenID Simple Registration Extension-1.0
- Authentication; SAML-2.0
- Authentication; RADIUS
- Authentication; Kerberos-5
- Authentication; OpenID Authentication-2.0
- Authentication; OpenID Authentication-1.1
- Authorization; OAuth-2.0
- Infra. Identity Mgmt.; IPsec
- Provisioning; SPML-2.0
- Provisioning; SCIM Core Schema-2.0
- Authentication; OpenID Provider Authentication Policy Extension-1.0
- Provisioning; SCIM-2.0
- Provisioning; SCIM REST API-2.0

- Provisioning; SCIM Targeting-2.0
- Authentication; OpenID Connect-1.0
- Authentication; OpenID Connect Basic Client Profile-1.0
- Authentication; OpenID Connect Implicit Client Profile-1.0
- Authentication; OpenID Connect Discovery-1.0
- Authentication; OpenID Connect Dynamic Client Registration-1.0
- Authentication; OpenID Connect Standard-1.0
- Authentication; OpenID Connect Messages-1.0
- Authentication; OpenID Connect Session Management-1.0
- Authorization; OpenID Connect OAuth 2.0 Multiple Response Type Encoding Practices-1.0

### 3.15.5 Analysis notes

- VPN standards are relevant for this use case.

### 3.15.6 Possible GAPs identified

## 3.16 Use Case 16: Offload Identity Management to External Business Entity

### 3.16.1 Short description

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.

### 3.16.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.16.3 Featured Cloud Deployment or Service Models

| **Featured Cloud Deployment Models** | | | | | **Featured Cloud Service Models** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.16.4 Relevant applicable standards

- Account / Attribute Mgmt.; OpenID Attribute Exchange-1.0
- Fed. Identity Mgmt.; WS-Federation-1.2
- Account / Attribute Mgmt.; OpenID Simple Registration Extension-1.0
- Authentication; SAML-2.0
- Authentication; OpenID Authentication-2.0
- Authentication; OpenID Authentication-1.1
- Authorization; OAuth-2.0
- Provisioning; SPML-2.0
- Provisioning; SCIM Core Schema-2.0
- Authentication; OpenID Provider Authentication Policy Extension-1.0
- Provisioning; SCIM-2.0
- Provisioning; SCIM REST API-2.0
- Provisioning; SCIM Targeting-2.0
- Authentication; OpenID Connect-1.0

- Authentication; OpenID Connect Basic Client Profile-1.0
- Authentication; OpenID Connect Implicit Client Profile-1.0
- Authentication; OpenID Connect Discovery-1.0
- Authentication; OpenID Connect Dynamic Client Registration-1.0
- Authentication; OpenID Connect Standard-1.0
- Authentication; OpenID Connect Messages-1.0
- Authentication; OpenID Connect Session Management-1.0
- Authorization; OpenID Connect OAuth 2.0 Multiple Response Type Encoding Practices-1.0

### 3.16.5 Analysis notes

- Authorization aspects are relevant for this use case.
- Project CAS
- Reference to: Step-up use case 11 and use case 12.
- Granularity issue: same app, depending on IdP and credentials, might make you can do different things in the application, so in fact result into different privileges in the app.

### 3.16.6 Possible GAPs identified

## 3.17 Use Case 17: Per Tenant Identity Provider Configuration

### 3.17.1 Short description

Show the need for cloud tenants to securely manage cloud services using automated tools rather than navigating and manually configuring each service individually.

### 3.17.2 Covered Identity Management Categories

| **Infra. Identity Est.** | **Identity Mgmt.** | | | **Authentication** | | | **Authorization** | **Account / Attribute Mgmt.** | | **Security Tokens** | **Governance** | **Audit & Compliance** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ***Gen.*** | ***IIM*** | ***FIM*** | ***Gen.*** | ***SSO*** | ***Multi-Factor*** | | ***Gen.*** | ***Provisioning*** | | | |
| | P | | | | | | | P | | | | |

### 3.17.3 Featured Cloud Deployment or Service Models

| **Featured Cloud Deployment Models** | | | | | **Featured Cloud Service Models** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.17.4 Relevant applicable standards

- Fed. Identity Mgmt.; IMI-1.0
- Provisioning; SPML-2.0
- Provisioning; SCIM Core Schema-2.0
- Provisioning; SCIM-2.0
- Provisioning; SCIM REST API-2.0
- Provisioning; SCIM Targeting-2.0

### 3.17.5 Analysis notes

- Key is this use case is how to define a policy for all customers and apply this to all cloud providers (assuming there are different ones), so in effect provision to multiple cloud providers, set permissions and propagate those.

- Possible solutions are along the lines of adaptors per cloud provider or broker functions.

- Important aspects in this use case are resource management and authorization

### 3.17.6 Possible GAPs identified

## 3.18 Use Case 18: Delegated Identity Provider Configuration

### 3.18.1 Short description

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.

### 3.18.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.18.3 Featured Cloud Deployment or Service Models

| Featured Cloud Deployment Models | | | | | Featured Cloud Service Models | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *None* | *Private* | *Public* | *Community* | *Hybrid* | *None* | *SaaS* | *PaaS* | *IaaS* | *Other* |
| X | | | | | | X | | | |

### 3.18.4 Relevant applicable standards

- Fed. Identity Mgmt.; IMI-1.0

### 3.18.5 Analysis notes

- Authentication, authorization and access management are key aspects.
- ISO WG on Access Management might provide us with relevant input.

### 3.18.6 Possible GAPs identified

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

### 3.19.1 Short description

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

### 3.19.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.19.3 Featured Cloud Deployment or Service Models

| **Featured Cloud Deployment Models** | | | | | **Featured Cloud Service Models** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.19.4 Relevant applicable standards

- Account / Attribute Mgmt.; OpenID Attribute Exchange-1.0
- Authorization; XACML-3.0
- Fed. Identity Mgmt.; WS-Federation-1.2
- Infra. Identity Mgmt.; KMIP-1.1
- Account / Attribute Mgmt.; OpenID Simple Registration Extension-1.0
- Authentication; SAML-2.0
- Provisioning; CIMI-1.0.0
- Authentication; OpenID Authentication-2.0
- Authorization; OAuth-2.0
- Authentication; OpenID Provider Authentication Policy Extension-1.0
- Privacy; P3P-1.1
- Virtual Machines; OVF-2.0
- Privacy; PMRM-1.0
- Authentication; OpenID Connect-1.0
- Authentication; OpenID Connect Basic Client Profile-1.0
- Authentication; OpenID Connect Implicit Client Profile-1.0

- Authentication; OpenID Connect Discovery-1.0
- Authentication; OpenID Connect Dynamic Client Registration-1.0
- Authentication; OpenID Connect Standard-1.0
- Authentication; OpenID Connect Messages-1.0
- Authentication; OpenID Connect Session Management-1.0
- Authorization; OpenID Connect OAuth 2.0 Multiple Response Type Encoding Practices-1.0

### 3.19.5 Analysis notes

- Relevant aspects are audit and compliance, access control, cloud storage and privacy
- Geography seems very relevant within the context of this use case – who can / has access to videos.[compliance aspect]
- Difficult to draw a clean line between identity and access.
- If one can audit in the cloud e.g. as simple as the accessing a piece of blog data, one has basically the foundation for auditing other data
- Within an enterprise there are compliance regulations; within a cloud no standards exist to audit and proof compliance
- Reporting access management type events; audit requirements: timestamp, identity, identity of resource involved (e.g. document, storage device), if encryption is applied (how it is protected)
- There is a need for standardized audit type events and reports
- 3 cloud audit spaces: (i) computing (ii) storage (iii) network
- Cloud standards such as SNIA not capable of providing audit functions yet. DMTF CIMI is considering this; worth considering the log format.
- The syslog type logging format seems useable as a log format. E.g. SNIA and CMIM use this too.
- Alignment of data model and topology is required
- Auditing aspects from a hardware perspective: on which server is e.g. a virtual image running
- Relevant areas to this subject are: audit reports and privacy information obfuscation
- Include key life cycle management aspects in audit events

### 3.19.6 Possible GAPs identified

- reference to audit already mentioned in previous use case analysis

- Standard interface to assign policies to different resources / assets in the cloud
- There are means of policy expression, but no interface to assign, identify, manage or track policy to assets
- policies applicable to the life cycle of an asset need to be included in audit information
- Within a cloud context no standards exist to audit and proof compliance
- Everything that has to do with asset management; there should be a provision for auditing

## 3.20 Use Case 20: Government Provisioning of Cloud Services

### 3.20.1 Short description

Show how authorized government personnel could be granted access and assigned appropriate privileges to configure and provision a cloud service.

### 3.20.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.20.3 Featured Cloud Deployment or Service Models

| Featured Cloud Deployment Models | | | | | Featured Cloud Service Models | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *None* | *Private* | *Public* | *Community* | *Hybrid* | *None* | *SaaS* | *PaaS* | *IaaS* | *Other* |
| X | | | | | | X | | | |

### 3.20.4 Relevant applicable standards

- Authorization; XACML-3.0
- Authentication; SAML-2.0
- Provisioning; SPML-2.0
- Provisioning; SCIM Core Schema-2.0
- Provisioning; SCIM-2.0
- Provisioning; SCIM REST API-2.0
- Provisioning; SCIM Targeting-2.0

### 3.20.5 Analysis notes

- Main point is how to authorize government personnel when outsources to a 3rd party.
- Relevant aspects are provisioning, authorization, access control and identity proofing
- Relevant link: New Electronic Authentication Guidelines for today's challenge of remote-user authentication - http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910006
- Activity logs: billing, metering

- Template: specification of the configuration of the service one is requesting, e.g. bandwidth, CPU, memory, SLA aspects, etc.
- DMTF is touching on this in management standards or protocols
- Customers want to be able to perform clear comparisons between cloud offerings, with respect to SLA, SLM, etc.

### 3.20.6 Possible GAPs identified

- Audit requirements for human and service based (non-security related) actions

## 3.21 Use Case 21: Mobile Customers' Identity Authentication Using a Cloud provider

### 3.21.1 Short description

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.

### 3.21.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.21.3 Featured Cloud Deployment or Service Models

| **Featured Cloud Deployment Models** | | | | | **Featured Cloud Service Models** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.21.4 Relevant applicable standards

- Authentication; SAML-2.0
- Authorization; OAuth-2.0
- Infra. Identity Mgmt.; WS-Trust-1.4
- Privacy; PMRM-1.0

### 3.21.5 Analysis notes

- Focus of this use case is on customer instead of the employee of a company.
- In mobile, the use of the device in MFA is the distinguishing characteristic
- Device id would be one of the attributes/factors involved
- Such use requires a device registration process (possibly more than one per account)

- Process flow for the use case should probably include the registration and other process steps
- Unclear if there is a standard for device registration (profile)
- Various keywords from the use case (device, secure hardware, registration, MFA). Research required based on those keywords to identify other potentially relevant standards
- This use case may have applicability to healthcare scenarios, so there might be some relevant healthcare standards – (reference to xspa profiles)
- Geo-locations are relevant as customers in the mobile space can be located in different places. How to define geo-location? lat-long may not be sufficient. Different granularities of geo-location might be required. This is also important with respect to audit.
- Other identities or factors involved e.g. SIM, hardware ID, etc. These factors can be used to increase level of trust.
- Mutual authentication desirable for security standards in cloud context.

### 3.21.6 Possible GAPs identified

- Mutual authentication for security standards
- No standard for mobile device registration; devices have different combinations of IDs (e.g. SIM ids, chip ids, IMEI) – this is manufacturer dependent. Laptops with TPM.
- Geo-location: authentication standards and device management and trackings standards; not aware of geo-location as a function or part of that.

## 3.22 Use Case 22: Cloud-based Two-Factor Authentication Service

### 3.22.1 Short description

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.

### 3.22.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.22.3 Featured Cloud Deployment or Service Models

| Featured Cloud Deployment Models | | | | | Featured Cloud Service Models | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *None* | *Private* | *Public* | *Community* | *Hybrid* | *None* | *SaaS* | *PaaS* | *IaaS* | *Other* |
| X | | | | | | X | | | |

### 3.22.4 Relevant applicable standards

- Infra. Identity Mgmt.; TOTP
- Infra. Identity Mgmt.; HOTP

### 3.22.5 Analysis notes

- Relevant is Two-Factor Authentication, smart card and token standards.
- authN standards consider to have profile to support multi-factor authentication, as customers will request this for performing previleged actions.

### 3.22.6 Possible GAPs identified

## 3.23 Use Case 23: Cloud Application Identification using Extended Validation Certificates

### 3.23.1 Short description

Shows the value of providing validatable identification of the Cloud Provider/SaaS application to the user or consumer using Extended Validation (EV) certificates.

### 3.23.2 Covered Identity Management Categories

| **Infra. Identity Est.** | **Identity Mgmt.** | | | **Authentication** | | | **Authorization** | **Account / Attribute Mgmt.** | | **Security Tokens** | **Governance** | **Audit & Compliance** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ***Gen.*** | ***IIM*** | ***FIM*** | ***Gen.*** | ***SSO*** | ***Multi-Factor*** | | ***Gen.*** | ***Provisioning*** | | | |
| | P | | | | | | | P | | | | |

### 3.23.3 Featured Cloud Deployment or Service Models

| **Featured Cloud Deployment Models** | | | | | **Featured Cloud Service Models** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.23.4 Relevant applicable standards

- Authentication; SAML-2.0
- Infra. Identity Mgmt.; X.509-3.0
- Assurance; EV certificates-1.4

### 3.23.5 Analysis notes

- Other PKI standards might apply.

- An Extended Validation Certificate (EV) is an X.509 public key certificate issued according to a specific set of identity verification criteria. These criteria require extensive verification of the requesting entity's identity by the certificate authority (CA) before a certificate is issued. Certificates issued by a CA under the EV guidelines are not structurally different from other certificates (and hence provide no stronger cryptography than other, cheaper certificates), but are designated with a CA-specific policy identifier so that EV-aware software can recognize them.

- The criteria for issuing EV certificates are defined by the Guidelines for Extended Validation Certificates, currently  (as of Nov 2010) at version 1.3. The guidelines[1] are produced by the CA/Browser Forum, a voluntary organization whose members include leading CAs and vendors of Internet software, as well as representatives from the legal and audit professions
- EV certificates is basically a trust elevator compared to regular certificates
- When hosting an app in public cloud managed by a different entity, how are the certificates managed; are they still ev-certs?

### 3.23.6 Possible GAPs identified

- Can (EV) certs be used in cloud environments using one domain for multiple clients? E.g. EV cert for customer1.office365.com, EV cert for customer2.office365.com, etc.
- Basic point in this use case: when connecting to a cloud based service, how does one know you are actually connected to the cloud service? There seems to be a need for trust when connecting to cloud services. This should be valid for any protocol and / or non-browser based to.

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

### 3.24.1 Short description

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.

### 3.24.2 Covered Identity Management Categories

| **Infra. Identity Est.** | **Identity Mgmt.** | | | **Authentication** | | | **Authorization** | **Account / Attribute Mgmt.** | | **Security Tokens** | **Governance** | **Audit & Compliance** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ***Gen.*** | ***IIM*** | ***FIM*** | ***Gen.*** | ***SSO*** | ***Multi-Factor*** | | ***Gen.*** | ***Provisioning*** | | | |
| | P | | | | | | | P | | | | |

### 3.24.3 Featured Cloud Deployment or Service Models

| **Featured Cloud Deployment Models** | | | | | **Featured Cloud Service Models** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.24.4 Relevant applicable standards

- Provisioning; CMDBf-1.0.1
- Infra. Identity Mgmt.; TPM-1.2

### 3.24.5 Analysis notes

- Relevant standards areas are in auditing and hardware based identity.
- Audit standards that map to regulatory and compliance frameworks and policies
- Proof of execution: evidence that software
- Persistent hardware IDs being exposed to software; profiles or specifications that build on existing standards for hardware-based identity (e.g. TCG TPM1.2 specs) and exposing these hardware-identities
- @editor: reference use case from redhat on IDs virtualized resources

- Provider should track these IDs of virtualized resources, also when moving these. Use a e.g. CMDB to store these IDs.

### 3.24.6 Possible GAPs identified

- Profiles or specifications that build on existing standards for hardware-based IDs and propagated and tracked in hypervisor and VMs and exposing these

## 3.25 Use Case 25: Inter-cloud Document Exchange and Collaboration

### 3.25.1 Short description

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.

### 3.25.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.25.3 Featured Cloud Deployment or Service Models

| Featured Cloud Deployment Models | | | | | Featured Cloud Service Models | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *None* | *Private* | *Public* | *Community* | *Hybrid* | *None* | *SaaS* | *PaaS* | *IaaS* | *Other* |
| X | | | | | | X | | | |

### 3.25.4 Relevant applicable standards

- Account / Attribute Mgmt.; OpenID Attribute Exchange-1.0
- Fed. Identity Mgmt.; IMI-1.0
- Governance; ebXML CPPA-2.0
- Infra. Identity Mgmt.; WS-ReliableMessaging-1.2
- Infra. Identity Mgmt.; WS-SecureConversation-1.4
- Account / Attribute Mgmt.; OpenID Simple Registration Extension-1.0
- Authentication; SAML-2.0
- Authentication; OpenID Authentication-2.0
- Authorization; OAuth-2.0
- Infra. Identity Mgmt.; WS-Trust-1.4
- Provisioning; SPML-2.0
- Provisioning; SCIM Core Schema-2.0
- Authentication; OpenID Provider Authentication Policy Extension-1.0
- Provisioning; SCIM-2.0
- Provisioning; SCIM REST API-2.0

- Provisioning; SCIM Targeting-2.0
- Authentication; OpenID Connect-1.0
- Authentication; OpenID Connect Basic Client Profile-1.0
- Authentication; OpenID Connect Implicit Client Profile-1.0
- Authentication; OpenID Connect Discovery-1.0
- Authentication; OpenID Connect Dynamic Client Registration-1.0
- Authentication; OpenID Connect Standard-1.0
- Authentication; OpenID Connect Messages-1.0
- Authentication; OpenID Connect Session Management-1.0
- Authorization; OpenID Connect OAuth 2.0 Multiple Response Type Encoding Practices-1.0

### 3.25.5 Analysis notes

- Distinction between Federated Identity operations and Provisioning
- Provisioning is CRUD operations on top of directories
- Federated Identity has a notion of a trusted identity providers
- Scenarios 1 and 3 relate to identity setup, and the associated attributes
- Scenario 2: re authorization to submit documents -- In identity terms, this depends on establishing/validating a match between a pre-existing identity in the receiver system, and a newly-provisioned identity triggered by the sender system, based on the matching of certain attributes associated with each of those two identities.
- Business relation with cloud provider; business puts documents at cloud provider; partner to work with these documents. Via email invite partner to access and work with the documents. Main point is setting up the channel between business and partner.
- When receiving an invite via email, what trust needs to be established before one can begin to engage in business
- Is there a way to setup a trust relationship from scratch?

### 3.25.6 Possible GAPs identified

- Setting up a trust relationship: starting from something small (e.g. an email) to start a trust relationship (invitation process)
- Using for this services to communicate what the mechanism would be to establish a certain trust level (referring to collaboration authorization service from the use case description)

## 3.26 Use Case 26: Identity Impersonation / Delegation

### 3.26.1 Short description

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.

### 3.26.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.26.3 Featured Cloud Deployment or Service Models

| **Featured Cloud Deployment Models** | | | | | **Featured Cloud Service Models** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.26.4 Relevant applicable standards

- Authorization; OAuth-2.0
- Infra. Identity Mgmt.; WS-Trust-1.4

### 3.26.5 Analysis notes

- Identity delegation / 'On behalf of' notion.
- Federation standards with attributes are relevant.
- Requirement for audit: should log the 'on behalf of', even over multi-layer delegations
- Delegation / 'on behalf of' scenarios:
  - multi-layer / multi-hup / multi-level delegation
- OAuth has some notion of the on-behalf-of: e.g. I have site with photo's; I can tell the print service to get the photo's through delegation of rights to the print service. Bound to single resource to a single use

- Should include access control to order to limit the intended use of the on-behalf-of

### 3.26.6 Possible GAPs identified

- Include delegation
- Scope limitation for delegation: Resource access limitation by time, operation, etc.

## 3.27 Use Case 27: Federated User Account Provisioning and Management for a Community of Interest (CoI)

### 3.27.1 Short description

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.

### 3.27.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.27.3 Featured Cloud Deployment or Service Models

| Featured Cloud Deployment Models | | | | | Featured Cloud Service Models | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.27.4 Relevant applicable standards

- Account / Attribute Mgmt.; IGF-CARML-1.0
- Provisioning; SPML-2.0
- Provisioning; SCIM Core Schema-2.0
- Provisioning; SCIM REST API-2.0
- Provisioning; SCIM Targeting-2.0

### 3.27.5 Analysis notes

- This use case is about the management of the data, not the actual use of the data

- Mapping, provisioning, synchronising attributes

- reference to attribute mapping / ldif (use case 4)

- Physical ID relation to digital ID

- What standards for biometric (e.g. iris, fingerprint, voice, face, presence) attributes exist (ISO SG27)? This could be good to specify / type attributes instead of creating blob-type attributes.
    - Reinforcing credentials (e.g. keyboard typing 'print').
- Use the same attribute names and categorization would be very beneficial. Most likely to see this within industries. Transform between attributes will happen (like schema transforms).

### 3.27.6 Possible GAPs identified

## 3.28 Use Case 28: Cloud Governance and Entitlement Management

### 3.28.1 Short description

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.

### 3.28.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.28.3 Featured Cloud Deployment or Service Models

| Featured Cloud Deployment Models | | | | | Featured Cloud Service Models | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.28.4 Relevant applicable standards

- Authorization; XACML-3.0
- Account / Attribute Mgmt.; IGF-CARML-1.0
- Provisioning; SPML-2.0
- Provisioning; SCIM Core Schema-2.0
- Provisioning; SCIM-2.0
- Provisioning; SCIM REST API-2.0
- Provisioning; SCIM Targeting-2.0

### 3.28.5 Analysis notes

- Spml and scim about exchange of info
- Xacml about expression of policy
- No expression of the result

- Standardize this? Or is this implementation?

### 3.28.6 Possible GAPs identified

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

### 3.29.1 Short description

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.

### 3.29.2 Covered Identity Management Categories

| Infra. Identity Est. | Identity Mgmt. | | | Authentication | | | Authorization | Account / Attribute Mgmt. | | Security Tokens | Governance | Audit & Compliance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Gen.* | *IIM* | *FIM* | *Gen.* | *SSO* | *Multi-Factor* | | *Gen.* | *Provisioning* | | | |
| | P | | | | | | | P | | | | |

### 3.29.3 Featured Cloud Deployment or Service Models

| **Featured Cloud Deployment Models** | | | | | **Featured Cloud Service Models** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***None*** | ***Private*** | ***Public*** | ***Community*** | ***Hybrid*** | ***None*** | ***SaaS*** | ***PaaS*** | ***IaaS*** | ***Other*** |
| X | | | | | | X | | | |

### 3.29.4 Relevant applicable standards

- Authorization; XACML-3.0
- Authorization; UMA-0.7

### 3.29.5 Analysis notes

- Need to better define users: are these customers, consumers, etc.?
- Users are able to dynamically delegate; how does this relate to data controllers / data processor concepts as understood within the privacy realm? Wording should be chosen carefully with respect to privacy definitions.
- Same as use case 26, item ‘scope’ controlled by the owner
- Similar to Google Docs, Office365, Skydrive, etc.
- Resource granular access delegation by resource owner; example Facebook

### 3.29.6 Possible GAPs identified

- Same as above; variation is need for user control for revocation, changes, etc. (especially when they have been chained).

# Appendix A. Acknowledgments

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

Participants:

Abbie Barbir, Bank of America
Jeffrey Broberg, CA Technologies
Carl Bunje, The Boeing Company
Milan Calina, First Point Global Pty Ltd.
Brian Campbell, Ping Identity Corporation
David Chadwick, Individual Member
Aradhna Chetal, The Boeing Company
Doron Cohen, SafeNet, Inc.
Sastry Dhara, Individual Member
Gines Dolera Tormo, NEC Corporation
Michele Drgon, Individual Member
Felix Gomez Marmol, NEC Corporation
Bob Gupta, Viometric, LLC
Tomas Gustavsson, PrimeKey Solutions AB
Patrick Harding, Ping Identity Corporation
Thomas Hardjono, M.I.T.
Hadass Harel, eBay, Inc.
Masum Hasan, Cisco Systems
ChengDong He, Huawei Technologies Co., Ltd.
Heather Hinton, IBM
Rainer Hoerbe, Individual Member
Gershon Janssen, Individual Member
Chris Kappler, PricewaterhouseCoopers LLP
David Kern, IBM
Kelvin Lawrence, IBM
Paul Lipton, CA Technologies
Paul Madsen, Ping Identity Corporation
Dimitar Mihaylov, SAP AG
Dale Moberg, Axway Software
Anthony Nadalin, Microsoft
John Newton, Alfresco Software
Dominique Nguyen, Bank of America
Guillaume Noe, Deloitte Consulting LLP
li peng, Huawei Technologies Co., Ltd.
Darren Platt, Symplified
Nick Pope, Thales e-Security
Donald Provencher, Bank of America
Martin Raepple, SAP AG
Christopher Ramstrom, CA Technologies
Darran Rolls, SailPoint Technologies
Matthew Rutkowski, IBM
Anil Saldhana, Red Hat

Richard Sand, Individual Member
Joe Savak, Rackspace Hosting, Inc.
Ziad Sawalha, Rackspace Hosting, Inc.
Mark Schertler, Axway Software
Suneet Shah, OpenIAM, LLC
Sean Shen, China Internet Network Information Center(CNNIC)
Jerry Smith, US Department of Defense (DoD)
Xiaonan Song, Primeton Technologies, Inc.
Scott Stark, Red Hat
Don Thibeau, Open Identity Exchange
Cathy Tilton, Daon
John Tolbert, The Boeing Company
David Turner, Microsoft
Steve VanTill, Security Industry Association
Colin Wallis, New Zealand Government
YanJiong WANG, Primeton Technologies, Inc.
Jeffrey Wheeler, Huawei Technologies Co., Ltd.
Frank Wray, Bank of America
Frank Wray, PricewaterhouseCoopers LLP:
Kevin Yu, Verizon Business
Aaron Zhang, Huawei Technologies Co., Ltd.

# Appendix B. Revision History

| Revision | Date | Editor | Changes Made |
|---|---|---|---|
| 01a | February 03, 2012 | Gershon Janssen | Initial draft version. |
| 01b | February 19, 2012 | Gershon Janssen | Added output of first pass on applicable standards for all use cases to the document. |
| 01c | May 14, 2012 | Gershon Janssen | Added output of gap analysis discussions. |
| 01d | May 18, 2012 | Gershon Janssen | Added draft output of F2F gap analysis discussions. No editorial clean-up and rewording. |
| 02 | April 1, 2013 | Gershon Janssen | Updated document with all gap analysis discussions output. |
| 03 | April 27, 2013 | Gershon Janssen | Added Acknowledgements section. |