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

Identity in the Cloud Outsourcing Profile 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-outsourcing/v1.0/cnprd01/IDCloud-outsourcing-v1.0-cnprd01.doc (Authoritative)

http://docs.oasis-open.org/id-cloud/IDCloud-outsourcing/v1.0/cnprd01/IDCloud-outsourcing-v1.0-cnprd01.html

http://docs.oasis-open.org/id-cloud/IDCloud-outsourcing/v1.0/cnprd01/IDCloud-outsourcing-v1.0-cnprd01.pdf

Previous version:

N/A

Latest version:

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

http://docs.oasis-open.org/id-cloud/IDCloud-outsourcing/v1.0/IDCloud-outsourcing-v1.0.html

http://docs.oasis-open.org/id-cloud/IDCloud-outsourcing/v1.0/IDCloud-outsourcing-v1.0.pdf

Technical Committee:

OASIS Identity in the Cloud TC

Chairs:

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

Editors:

Ginés Dólera Tormo (gines.dolera@neclab.eu), NEC Corporation
Félix Gómez Mármol (felix.gomez-marmol@neclab.eu), NEC Corporation

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 is intended to provide a profile for Identity Management outsourcing in Cloud Computing.

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-Outsourcing-v1.0]

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

Copyright © OASIS Open 2013. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

1 Introduction 5

1.1 References 5

2 Definitions 6

3 Use Cases 9

3.1 Use Case 2: Identity Provisioning 9

3.1.1 Short description 9

3.1.2 Relevant applicable standards 9

3.2 Use Case 4: Identity Configuration 9

3.2.1 Short description 9

3.2.2 Relevant applicable standards 9

3.3 Use Case 16: Offload Identity Management to External Business Entity 9

3.3.1 Short description 9

3.3.2 Relevant applicable standards 10

3.4 Use Case 17: Per Tenant Identity Provider Configuration 10

3.4.1 Short description 10

3.4.2 Relevant applicable standards 10

3.5 Use Case 18: Delegated Identity Provider Configuration 10

3.5.1 Short description 10

3.5.2 Relevant applicable standards 10

3.6 Use Case 20: Government Provisioning of Cloud Services 11

3.6.1 Short description 11

3.6.2 Relevant applicable standards 11

3.7 Use Case 26: Identity Impersonation / Delegation 11

3.7.1 Short description 11

3.7.2 Relevant applicable standards 11

3.8 Use Case 27: Federated User Account Provisioning and Management for a Community of Interest (CoI) 11

 Copyright © OASIS Open 2013. All Rights Reserved.

3.8.1 Short description 11
3.8.2 Relevant applicable standards 11
3.9 Use Case 29: User Delegation of Access to Personal Data in a Public Cloud 12
3.9.1 Short description 12
3.9.2 Relevant applicable standards 12
4 Standards 13
5 Challenges 14
5.1 Identity Provisioning 14
5.2 Delegated Authorization 14
5.3 Administration 14
5.4 Identity Confidentiality 14
Appendix A. Acknowledgments 15
Appendix B. Non-Normative Section 16
Appendix C. Revision History 17

 Copyright © OASIS Open 2013. All Rights Reserved.

1 Introduction

This document describes the various Identity Management use cases, challenges and applicable standards in the Identity Management Outsourcing in the Cloud Computing model.

Many of the services in the Internet require some identity-related functionality, such as authentication, information exchange, user attributes aggregation, etc. However, due to the diversity raised by cloud environments, it is hard for some enterprises or organizations to provide the required identity functionality needed for interacting with the different services.

Organizations or enterprises which do not have enough resources to deploy the required identity infrastructure could decide to externalize such identity management functionality. By outsourcing the identity management, those enterprises get another enterprise to be in charge of providing the required identity management functionality on their behalf.

1.1 References

[NIST-SP800-145]

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

[IDCLOUD-USECASES-1.0]

M.Rutkowski, *OASIS Identity In The Cloud Use Cases v1.0*, OASIS Standards Consortium, 08 May 2012. http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/cn01/IDCloud-usecases-v1.0-cn01.html

 Copyright © OASIS Open 2013. All Rights Reserved.

2 Definitions

Cloud Platform as a Service (PaaS)

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

Outsourcing identity

Outsourcing consists of an entity contracting with another company or person to do a particular function. Typically, the function being outsourced is considered non-core to the business. A company may want to outsource some functionality if it could be done more efficiently and therefore more cost-effectively, by other companies with specialized tools and facilities and specially trained personnel.

In this document we focus on outsourcing the identity management functionality. We consider outsourcing identity management to externalize all or part of the identity-related functionality. That includes authentication, information exchange, user attributes aggregation, etc. Due to the diversity raised by cloud environments, it is hard for some enterprises or organizations to deploy the required infrastructure needed to interact with the different services. Hence, organizations or enterprises which do not have enough resources to deploy the required identity infrastructure could decide to externalize such identity management functionality

Moreover, identity-related functionality not only includes implementing standard protocols for authentication, or authorization, such as SAML, OpenID or XACML, but it also requires establishing trust relationships with the different services, defining complex SLA agreements, exchanging public key certificates and so forth. Furthermore, the organizations should be adapted to the peculiarities of each service to interact with it.

By outsourcing the identity management, those enterprises get another enterprise to be in charge of providing the required identity management functionality on their behalf. The outsourcing vendor deploys the required identity infrastructure and establishes the necessary trust relationships with the different services making use of virtual Identity Providers in the cloud, which offer identity management functionality via SaaS. In this way, other enterprises or organizations could make use of that solution to access the different services without requiring being in charge of identity management.

Figure 1 represents an overview of a basic outsourcing scenario, where two enterprises externalize their identity-related functionality to the outsourcing service, which in turn is used as a bridge for accessing the different Internet services.

 Copyright © OASIS Open 2013. All Rights Reserved.

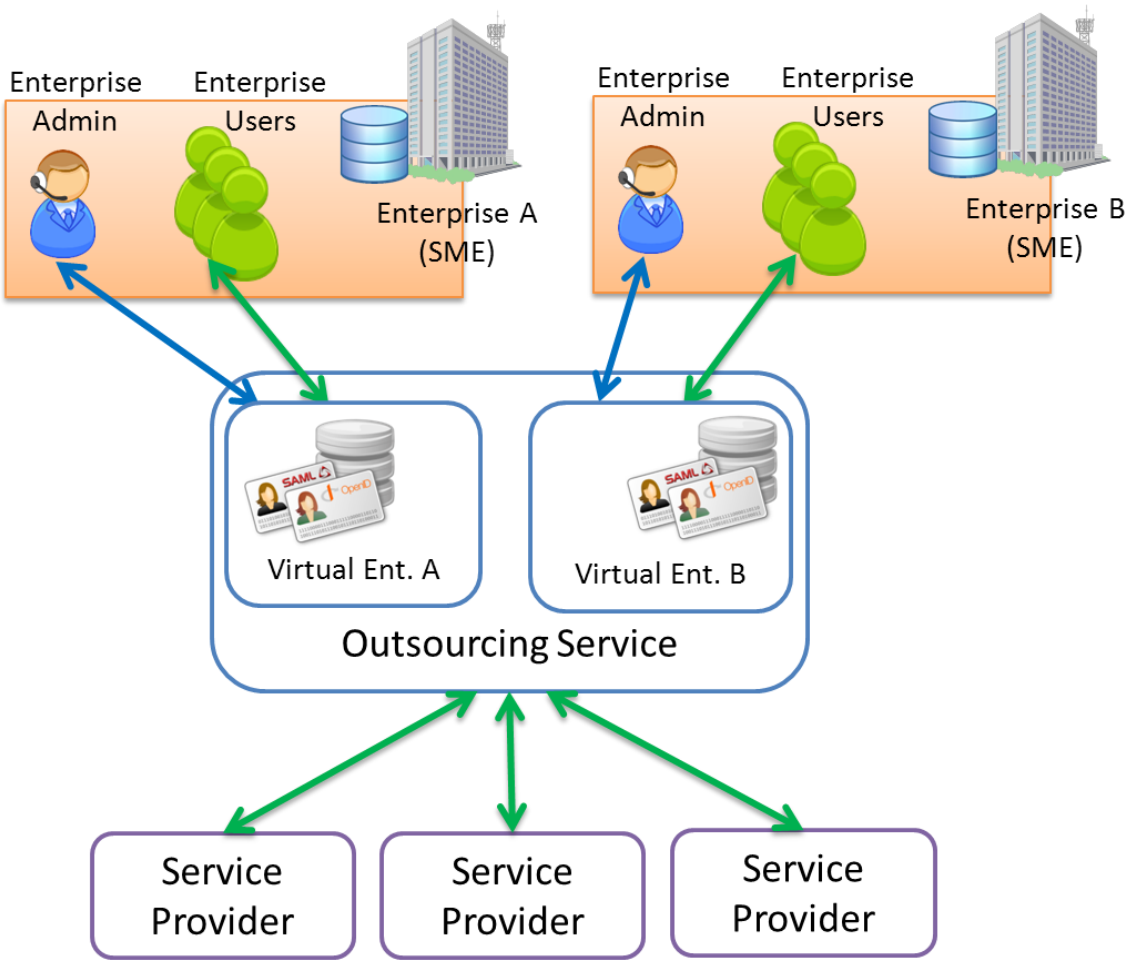

FIGURE 1. OUTSOURCING SERVICE SCENARIO OVERVIEW

As previously commented, identity-related functionality involves many different aspects. They are represented in Figure 2 and described below.

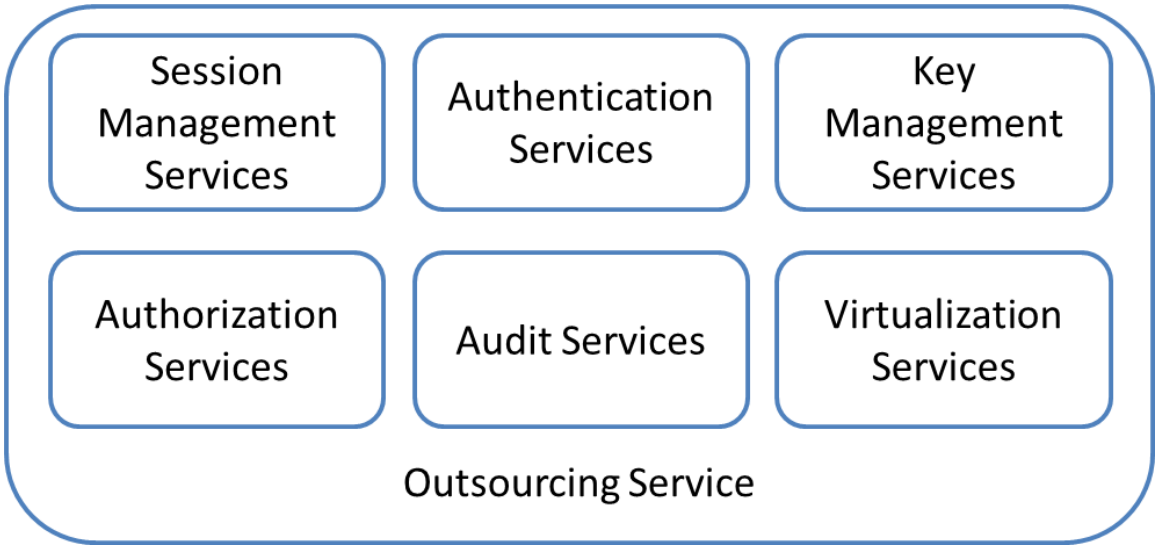

FIGURE 2. OUTSOURCING SERVICES

Copyright © OASIS Open 2013. All Rights Reserved.

- Session Management Services: Web sessions are established to maintain a state for each user of a web service. This form the basis for providing Single Sign-On (SSO).
- Authentication Services: The authentication process is often the aspect of security that is most visible to users. It validates that the user is actually who is claiming to be. There have been defined several authentication mechanisms, whose applicability depends on the requirements of the scenario.
- Key Management Services: An important part of outsourcing services is to manage trust relationships between the different providers. The outsourcing service establishes trust relationships by defining different Service-level agreements (SLA) and secured deploying certification services, such as public key infrastructure (PKI).
- Authorization Services: Besides authenticating the users, it is necessary to determine what actions are they able to perform over which resources.
- Audit Services: As many other identity management systems, outsourcing services have to incorporate an effective auditing system able to trace the relevant events happened in the system, so the users cannot deny performing an operation or initiating a transaction.
- Virtualization Services: The identity management functionality is virtualized for each company which wants to outsource this functionality. This allows the companies to manage their identity-related information without interferer with each other.

 Copyright © OASIS Open 2013. All Rights Reserved.

3 Use Cases

3.1 Use Case 2: Identity Provisioning

3.1.1 Short description

Feature the need support and manage customer policies for identity decommissioning including transitioning of affected resources to new identities. For extended description of this use case, please refer to **[IDCLOUD-USECASES-1.0]**

3.1.2 Relevant applicable standards

- Standards that provision uid's
- SPML
- OSLC (open-services.net) – open services for life cycle collaboration stds
- SCIM
- DMTF CIMI

3.2 Use Case 4: Identity Configuration

3.2.1 Short description

Feature the need for portable standards to configure identities in cloud applications and infrastructure (virtual machines, servers etc). For extended description of this use case, please refer to **[IDCLOUD-USECASES-1.0]**

3.2.2 Relevant applicable standards

- LDAP
- LDIF
- TOSCA
- OVF
- SAML

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

3.3.1 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

 Copyright © OASIS Open 2013. All Rights Reserved.

or its own institutional consumers and avoid directly managing identities (accounts) for those users. For extended description of this use case, please refer to **[IDCLOUD-USECASES-1.0]**

3.3.2 Relevant applicable standards

- SAML
- OpenID
- OpenID Connect
- OAuth
- WS-Federation
- SCIM
- SPML

3.4 Use Case 17: Per Tenant Identity Provider Configuration

3.4.1 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. For extended description of this use case, please refer to **[IDCLOUD-USECASES-1.0]**

3.4.2 Relevant applicable standards

- IMI
- SPML
- SCIM

3.5 Use Case 18: Delegated Identity Provider Configuration

3.5.1 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. For extended description of this use case, please refer to **[IDCLOUD-USECASES-1.0]**

3.5.2 Relevant applicable standards

- IMI

 Copyright © OASIS Open 2013. All Rights Reserved.

3.6 Use Case 20: Government Provisioning of Cloud Services

3.6.1 Short description

Show how authorized government personnel could be granted access and assigned appropriate privileges to configure and provision a cloud service. For extended description of this use case, please refer to **[IDCLOUD-USECASES-1.0]**

3.6.2 Relevant applicable standards

- SAML
- XACML
- SPML
- SCIM

3.7 Use Case 26: Identity Impersonation / Delegation

3.7.1 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. For extended description of this use case, please refer to **[IDCLOUD-USECASES-1.0]**

3.7.2 Relevant applicable standards

- WS-Trust

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

3.8.1 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. For extended description of this use case, please refer to **[IDCLOUD-USECASES-1.0]**

3.8.2 Relevant applicable standards

- SPML
- SCIM
- IGF

 Copyright © OASIS Open 2013. All Rights Reserved.

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

3.9.1 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. For extended description of this use case, please refer to **[IDCLOUD-USECASES-1.0]**

3.9.2 Relevant applicable standards

- UMA
- XACML

 Copyright © OASIS Open 2013. All Rights Reserved.

4 Standards

 Copyright © OASIS Open 2013. All Rights Reserved.

5 Challenges

5.1 Identity Provisioning

There is a need to manage lifecycle (Create, Read, Update and Delete) of users.

5.2 Delegated Authorization

There is a need to perform authorization processes. Furthermore, the authorization may be directed by other entities and hence the delegated authorization enabled. For example, a company wants to control the access of their users by their own methods and the authorization decisions should be delegated to it.

5.3 Administration

There is a need to enable administration capabilities so the different enterprises could manage their identity-related information.

5.4 Identity Confidentiality

There is a need to provide confidentiality services for identities. This includes capabilities such as Encryption, Decryption and Key Management.

Copyright © OASIS Open 2013. All Rights Reserved.

Appendix A. Acknowledgments

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

Participants:

Anil Saldhana, Red Hat

Scott Stark, Red Hat

Anthony Nadalin, Microsoft

David Turner, Microsoft

Matt Rutkowski, IBM

David Kern, IBM

Abbie Barbir, Bank of America

Dominique Nguyen, Bank of America

Thomas Hardjono, MIT

Jeffrey Broberg, CA Technologies

John Tolbert, The Boeing Company

Gines Dolera Tormo, NEC Corporation

Felix Gomex Marmol, NEC Corporation

Cathy Tilton, Daon

Dale Moberg, Axway Software

David Chadwick, Individual

Gershon Jannsen, Individual

Roger Bass, Individual

Michele Drgon, Individual

 Copyright © OASIS Open 2013. All Rights Reserved.

Appendix B. Non-Normative Section

 Copyright © OASIS Open 2013. All Rights Reserved.

Appendix C. Revision History

Revision	Date	Editor	Changes Made
01a	November 12, 2012	Ginés Dólera Tormo Félix Gómez Mármol	Initial draft version.
01b	January 21, 2013	Ginés Dólera Tormo Félix Gómez Mármol	Extended introduction and definition of the term 'outsourcing'
01c	April 29, 2013	Ginés Dólera Tormo Félix Gómez Mármol	Merge introduction and outsourcing definition. Extended outsourcing definition. Added Challenges

Copyright © OASIS Open 2013. All Rights Reserved.