Identity in the Cloud PaaS Profile Version 1.0

Committee Note Draft 02 / Public Review Draft 02

16 September 2013

Work Product URIs

This version:

http://docs.oasis-open.org/id-cloud/IDCloud-paas/v1.0/cnprd02/IDCloud-paas-v1.0-cnprd02.odt (Authoritative)

http://docs.oasis-open.org/id-cloud/IDCloud-paas/v1.0/cnprd02/IDCloud-paas-v1.0-cnprd02.html

http://docs.oasis-open.org/id-cloud/IDCloud-paas/v1.0/cnprd02/IDCloud-paas-v1.0-cnprd02.pdf

Previous version:

http://docs.oasis-open.org/id-cloud/IDCloud-paas/v1.0/cnprd01/IDCloud-paas-v1.0-cnprd01.odt (Authoritative)

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

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

Latest version:

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

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

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

Editor:

Anil Saldhana (anil.saldhana@redhat.com), Red Hat, Inc.

Related work:

This document is related to:

- *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.

Abstract:

This document is intended to provide a profile for Identity Management in Platform As A Service (PaaS) model of 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 Work Product 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 Work Product the following citation format should be used:

[IDCloud-PaaS-v1.0]

Identity in the Cloud PaaS Profile Version 1.0. 16 September 2013. OASIS Committee Note Draft 02 / Public Review Draft 02. http://docs.oasis-open.org/id-cloud/IDCloud-paas/v1.0/cnprd02/IDCloud-paas-v1.0-cnprd02.html.

Table of Contents

1 Introduction

This document describes the various Identity Management use cases, challenges and applicable standards in the Cloud Platform-As-A-Service (PaaS) model.

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

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]**

This document defines PaaS as follows:
The Cloud Platform-As-A-Service (PaaS) model is a Cloud Computing model where an application owner is able to deploy applications on to a managed platform. The platform management is not a responsibility of the application owner but the responsibility of the platform provider. The provider provides all facilities and tools for the application owner to deploy and manage the applications. The platform is composed of the necessary infrastructure such as servers, virtual machines, operating systems, storage, security services and compilers, to enable the deployment of applications.

We now look at a typical PaaS architecture that depicts components and services.

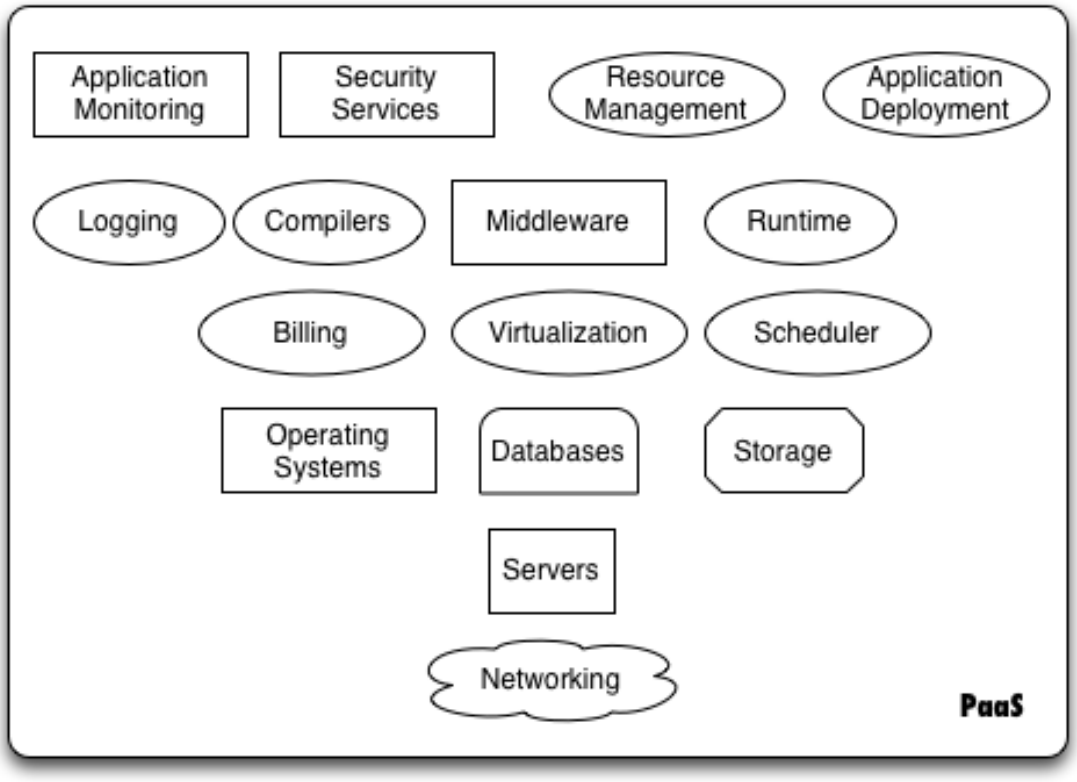

Figure 1: Typical PaaS Architecture

A PaaS architecture consists of the following:

- Application Deployment: PaaS environments provide deployment services for applications. This can optionally include packaging services.
- Application Runtime: PaaS environments provide a run time for applications. The runtime includes everything an application may need to execute and be available to users.
- Compilers: PaaS run times may perform application compilation. Compilers are provided in those situations.
- Application Monitoring: applications need to be monitored during their lifetimes for errors, health checks etc.
- Security Services: applications need security. Since applications require users, there is a need to identify the users. The Security Services can include authentication, provisioning and access control services.
- Resource Management: resources needed for the applications are managed via a resource management service.
- Logging/Auditing Services: Applications and Services in the PaaS environments may use the logging/auditing services for compliance purposes.
- Middleware: PaaS environments provide a collective set of software running on the operating system to manage and execute applications.
- Billing Services: Applications incur costs which are handled by the billing services.
- Virtualization: Cloud environments have virtualization.
- Scheduler: applications need to be scheduled for execution.
- Operating Systems: PaaS environments provide various Operating Systems under the covers.
- Databases: PaaS environments provide one or more database services for use by the applications.
- Storage: PaaS environments provide storage services for applications.
- Servers: PaaS environments include servers that are managed by the PaaS provider.
- Networking: PaaS provider will manage the networking required by the servers.

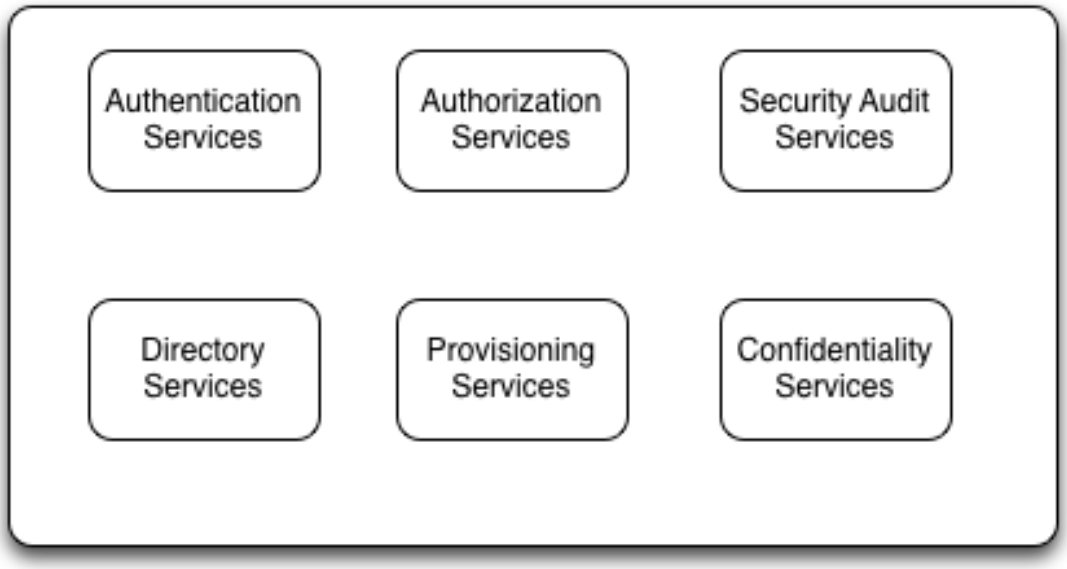

Figure 2: Security Services In PaaS

Figure 2 depicts the typical components or subsystems in the Security Services of PaaS. The components are not exhaustive.

- Authentication Services: are responsible for authenticating users to PaaS applications. Authentication Services need to take into consideration that the authenticating identity may be a federated identity.
- Authorization Services: are responsible for providing access control services to applications. This service may include Security Policies and Entitlement (access control privileges to users and applications) management.
- Security Audit Services: are responsible to include logging and other control mechanisms for compliance reasons.
- Directory Services: are responsible to provide look up services on users, roles, groups and attributes to applications and services inside the PaaS environment.
- Provisioning Services: are responsible to manage the lifecycle of Identity Objects such as Users, Roles, Groups, Attributes and other objects involved in Identity Management. Federated Identities need to be dealt by the Provisioning Services.
- Confidentiality Services: are responsible for providing confidentiality to applications and data in the PaaS environment. This may include encryption, decryption and key management services.

3 Use Cases

The following use cases are chosen from the IDCloud Use Case document **[IDCLOUD-USECASES-1.0]** based on relevance to PaaS.

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

3.1.2 Relevant applicable standards

- SAML
- WS-Trust
- OpenID
- oAuth
- OVF
- X.500
- LDAP
- IPsec
- RADIUS
- SPML
- SCIM

3.2 Use Case 3: Identity Audit

3.2.1 Short description

Feature the importance of auditing/logging of sensitive operations performed by users and administrators in the cloud. For extended description of this use case, please refer to **[IDCLOUD-USECASES-1.0]**

3.2.2 Relevant applicable standards

- CloudAudit
- ISO 27017

3.3 Use Case 4: Identity Configuration

3.3.1 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 **[ID-CLOUD-USECASES-1.0]**

3.3.2 Relevant applicable standards

- LDAP
- LDIF
- TOSCA
- OVF
- SAML

3.4 Use Case 5: Middleware Container in a Public Cloud

3.4.1 Short description

Show how cloud identities need to be administered and accounted for in order to manage middleware containers and their applications. For extended description of this use case, please refer to **[ID-CLOUD-USECASES-1.0]**

3.4.2 Relevant applicable standards

- SAML
- OpenID
- JavaEE
- OVF

3.5 Use Case 6: Federated SSO and Attribute Sharing

3.5.1 Short description

Feature the need for Federated Single Sign-On (F-SSO) across multiple cloud environments. For extended description of this use case, please refer to **[IDCLOUD-USECASES-1.0]**

3.5.2 Relevant applicable standards

- SAML
- XACML
- OpenID
- OpenID Connect
- oAuth
- UMA
- IMI
- WS-Trust

3.6 Use Case 10: Cloud Tenant Administration

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

3.6.2 Relevant applicable standards

- SAML
- OpenID
- oAuth
- CDMI

3.7 Use Case 11: Enterprise to Cloud SSO

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

3.7.2 Relevant applicable standards

- SAML
- OpenID
- OpenID Connect
- oAuth
- SPML
- SCIM

3.8 Use Case 17: Per Tenant Identity Provider Configuration

3.8.1 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]**

3.8.2 Relevant applicable standards

- IMI
- SPML
- SCIM

3.9 Use Case 18: Delegated Identity Provider Configuration

3.9.1 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]**

3.9.2 Relevant applicable standards

- IMI

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

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

3.10.2 Relevant applicable standards

- SAML
- OpenID
- OpenID Connect
- oAuth
- WS-Federation
- PMRM
- P3P
- OVF
- XACML
- SNIA
- CMIM
- KMIP

3.11 Use Case 22: Cloud-based Two-Factor Authentication Service

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

3.11.2 Relevant applicable standards

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

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

3.12.2 Relevant applicable standards

- SAML
- EV certificates
- X.509

4 Challenges

4.1 Federated Identity Support

There is a need to support Federated Identities in a PaaS model.

4.2 Identity Management Provisioning

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

4.3 Identity Audit

There is a need to audit operations performed by an Identity in a PaaS model.

4.4 Authorization

There is a need to perform authorization of resources and applications by users and processes.

4.5 Identity Confidentiality

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

5 Standards

The standards that are applicable to Platform-As-A-Service are divided into the following sections.

5.1 Federated Identity Standards

The following OASIS standards for Federated Identity are applicable:

- OASIS SAML
- OASIS WS-Trust and WS-Federation

5.2 Identity Management Provisioning

The following OASIS Standards for Identity Management provisioning are applicable:

- OASIS SPML

5.3 Authorization

The following OASIS Standard for Authorization is applicable:

- OASIS XACML

The following IETF Standard for Authorization is applicable:

- IEFT OAuth2

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

Appendix B Revision History

Revision	Date	Editor	Changes Made
01a	October 01, 2012	Anil Saldhana	Initial draft version.
01b	October 26,2012	Anil Saldhana	Changes based on Feedback
01f	February 4, 2013	Anil Saldhana	– Added Federated Identity concerns to Authentication and Provisioning Services – Expanded the Challenges Section
01g	April 26, 2013	Anil Saldhana	– Acknowledgements
01h	September 16, 2013	Anil Saldhana	– Removed the use case on Impersonation that was contentious.

