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

Mobile Cloud Identity Profile Version 1.0

Committee Note 01

05 August 2013

Specification URIs

This version:

http://docs.oasis-open.org/id-cloud/IDCloud-mobile/v1.0/cn01/IDCloud-mobile-v1.0-cn01.doc (Authoritative)
http://docs.oasis-open.org/id-cloud/IDCloud-mobile/v1.0/cn01/IDCloud-mobile-v1.0-cn01.html
http://docs.oasis-open.org/id-cloud/IDCloud-mobile/v1.0/cn01/IDCloud-mobile-v1.0-cn01.pdf

Previous version:

N/A

Latest version:

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

Anil Saldhana (Anil.Saldhana@redhat.com), Red Hat
Dominique Nguyen (dominique.v.nguyen@bankofamerica.com), Bank of America
Chris Kappler (chris.kappler@pwc.be), PricewaterhouseCoopers LLP

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 Mobile Identity Management.

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-mobile-v1.0]

Mobile Cloud Identity Profile Version 1.0. 05 August 2013. OASIS Committee Note 01. http://docs.oasis-open.org/id-cloud/IDCloud-mobile/v1.0/cn01/IDCloud-mobile-v1.0-cn01.html.

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

Table of Contents

1 Introduction

This document describes the consumers' mobile device authentication as an additional strong authentication use case, challenges and applicable standards in the Cloud -As-A-Service (*aaS) model.

1.1 References (non-normative)

[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

[NIST-SP800-164]
L. Chen, J. Franklin, A/ Regenshcheid, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), Recommendations of the National Institute of Standards and Technology (NIST) - Computer Security Division – Computer Security Resource Center (CSRC), October 2012. http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.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 computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. **[NISTSP800-145]**

A Device Owner is an entity that has purchased and maintains ownership of a mobile device. **[NISTSP800-164]**
An Information Owner is an entity whose information is stored and/or processed on a device. An Information Owner can be an application-specific provider, a digital product provider, or an enterprise that allows access to resources from mobile devices, for example. Every mobile device has a single Device Owner and one or more Information Owners. **[NISTSP800-164]**

Device integrity is the absence of corruption in the hardware, firmware and software of a device. A mobile device can provide evidence that it has maintained device integrity if the state of the device can be shown to be in a state that is trusted by a relying party. A device has integrity if its software, firmware, and hardware configurations are in a state that is trusted by a relying party. The mechanism for communicating this trusted state is through one or more assertions that the Device Owner allows a device to make to the Information Owner. A device may establish a unique device identity for the purpose of device authentication. Mobile devices may use assertions to represent the state of firmware as either verified or unverified, the state of an OS as either validated or not, the state of file encryption as either on or off, the state of the microphone as either on or off, etc. **[NISTSP800-164]**

A device may establish a unique device identity for the purpose of device authentication.

We now look at a typical Mobile Device identity interaction with the Cloud as an Information owner.

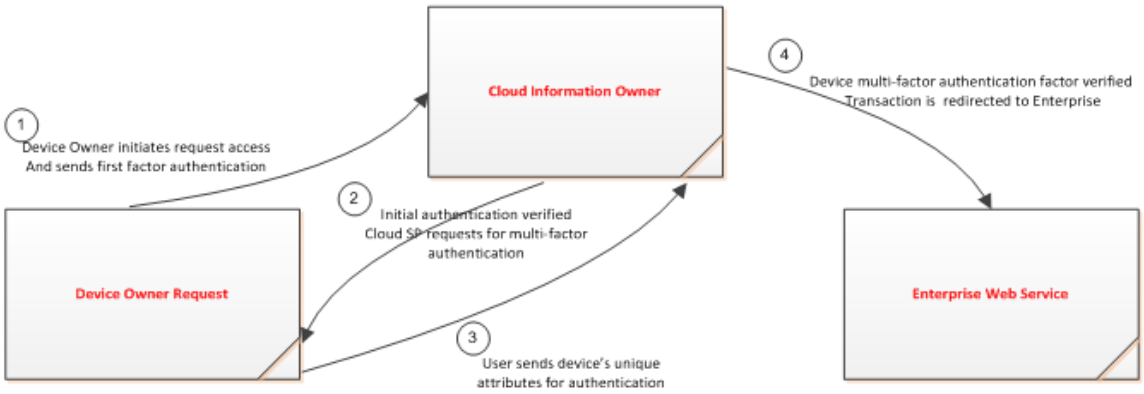

FIGURE 1 : INTERACTION BETWEEN MOBILE USERS (USING MOBILE UNIQUE ATTRIBUTES AS MULTI-FACTOR AUTHENTICATION) AND CLOUD SERVICE

Authentication scenario sequence includes:

1. A Mobile client logs on to the Financial Institution's (FI) on-line service website via mobile device browser.
2. Based on pre-arrangement, the Mobile client is directed to the Cloud authentication-hosting site.
3. The Mobile client enters credential for authentication.
4. Mutual authentication is invoked and secure channel is established to secure authentication information and attributes passed over wireless network.
5. Cloud authentication service provider validates the Mobile client credential (user credential and device credential (mobile phone number, other mobile device's unique attributes).
6. The Mobile client is authenticated and passed forward to the banking system to allow access to the system to conduct financial transaction.
7. Secure connection maintains throughout the session.
8. The Mobile client completes transaction and logs off.
9. Secure channel terminates.

3 Use Cases

3.1 Use Case 21: Mobile Customers' Identity Authentication Using Cloud Provider

3.1.1 Short description

This document demonstrates the need to have a standard secure identity authentication to authenticate mobile consumer user that exists in Cloud-based Identity and Access Management services offering identity proofing, credential management, strong authentication, single sign-on, and provisioning solutions when Cloud –based identity service is used as an intermediary between a consumer and a business enterprise.

3.1.2 Relevant applicable standards

- SAML
- OAuth
- XSPA
- WS-Trust
- PMRM

4 Challenges

4.1 Federated Identity Support

There is a need to support Federated Identities in any *aaS model.

4.2 Authorization

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

4.3 Secure connections

There is a need to ensure secure connection between Mobile Device, Cloud Information Owner and Enterprise Application.

4.4 Mobile User Authentication and Device Registration

There is a need to authenticate the mobile user.

One potential solution is as follows:

The goal is to identify a user using a secure channel. Sending a hash sets up the channel. The hash is a combination of the phone IMEI Number and the SIM card serial number. The reason these attributes are used is because they are common to all manufacturers and all carriers. They can also be obtained in the same manner independent of a manufacturer and carrier. The hashing is done so none of the info is sent as clear text over a carrier.

There's 2 ways of provisioning:

- If the device is company owned, then the hash result is directly inserted in the system.
- If the device is not company owned, then the hash is sent out at first installation by a secure channel.

Once a secure channel is established user authentication is done by means of a certificate and pin.

5 Standards

The standards that are applicable to *-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
- OASIS XSPA profile of SAML

5.2 Identity Management Provisioning

The following OASIS Standards for Identity Management provisioning are applicable:

- OASIS SPML

5.3 Authorization

The following OASIS Standards for Authorization are applicable:

- OASIS OAuth
- OASIS XACML

Appendix A. Acknowledgments

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

Participants:

Anil Saldhana, Red Hat

Anthony Nadalin, Microsoft

David Turner, Microsoft

Matt Rutkowski, IBM

David Kern, IBM

Chris Kappler, Pricewaterhousecoopers

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
1.0 a	May 13, 2013	Anil Saldhana and Dominique Nguyen	• Initial Version with content from Dominique
1.0b	June 10,2013	Chris Kappler	• Mobile User Authentication and Device Registration

