b

Enabler Release Definition for OMA Web Services Network Identity (OWSER NI) Enabler

Candidate Version 1.0 – 20 Dec 2005

Open Mobile Alliance

OMA-ERELD-OWSER_NI-V1_0-20051220-C

Contents

Tables

1. Scope

The scope of this document is limited to the Enabler Release Definition of OWSER NI according to OMA Release process and the Enabler Release specification baseline listed in section 0.

2. References

2.1 Normative References

[IOPPROC] “OMA Interoperability Policy and Process”, Version 1.1, Open Mobile Alliance™, OMA-IOP-Process-V1_1, URL:http://www.openmobilealliance.org/

[RFC2119] “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt

[OWSER NI FF] “OMA Web Services Network Identity Enabler (OWSER NI): Federation Framework”, Version 1.0, Open Mobile Alliance™, OMA-TS-OWSER_NI_FF-V1_0, URL:http://www.openmobilealliance.org/

[OWSER NI WSF] “OMA Web Services Network Identity Enabler (OWSER NI): Identity Web Services Framework”, Version 1.0, Mobile Alliance™, OMA-TS-OWSER-NI-WSF-V1_0, URL:http://www.openmobilealliance.org/

[OWSER NI AD] “OMA Web Services Network Identity Enabler (OWSER NI): Architecture”, Version 1.0, Open Mobile Alliance™, OMA-AD-OWSER_NI-V1_0, URL:http://www.openmobilealliance.org/

[NI REQ] “MWS Identity Management (OWSER NI) Requirements, Version 1.1”, Open Mobile Alliance™, OMA-RD-OWSER-NI-V1_1, URL:http://www.openmobilealliance.org/

2.2 Informative References

[LAP] “Liberty Alliance Version 1.1 Specification Suite”, January 2003, available at http://www.projectliberty.org/specs/archive/v1_1/liberty-specifications-v1.1.zip

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

The formal notation convention used in section 8 to formally express the structure and internal dependencies between specifications in the Enabler Release specification baseline is detailed in [IOPPROC].

3.2 Definitions

Account A formal business agreement for providing regular dealings and services between a Principal and Service Providers. (Source: [Liberty-Glossary])

Enabler Release Collection of specifications that combined together form an enabler for a service area, e.g. a download enabler, a browsing enabler, a messaging enabler, a location enabler, etc. The specifications that are forming an enabler should combined fulfil a number of related market requirements.

Minimum Functionality Description Description of the guaranteed features and functionality that will be enabled by implementing the minimum mandatory part of the Enabler Release.

Assertion A statement about a Principal.

Attribute An Attribute is a characteristic that describes a Principal.

Attribute Provider A special type of Service Provider, whose service is to provide Attributes about a Principal. In this document an Attribute provider is an ID-WSF-enabled Web Service Provider

Attribute Sharing See Attribute Transfer.

Attribute Transfer Transmission of a Principal’s Attribute from an Entity (i.e. an Attribute Provider) that manages it, on behalf of the Principal, to an Entity that requests it (e.g. a Service Provider).

Authentication The process of verifying an Identity claimed by (or for) a Principal.

Authentication Assertion An Assertion that can be sent from one Identity Provider (or an Identity Broker) to another Provider, which describes a successful Authentication of a Principal. An Authentication Assertion may also contain information such as for how long the Assertion is valid. An Authentication Assertion will also often include an Authentication Context, to notify the Provider what form of Authentication was used.

Authentication Context The set of parameters (time, location, transaction value, etc.) within which a specific authentication event is acceptable, emphasising that a single authentication event may need to be re-established, perhaps with different mechanisms or classes of mechanisms, when some parameter changes.

Authorisation A right or permission that is granted to a system Entity to access a system resource, or the process of granting the right or permission [RFC 2828].

Business Agreement Business agreements are formal agreements (contracts) between parties in the Identity Management Circle of Trust, documenting binding commitments between the parties with respect to aspects such as mutual confidence (e.g. business standards, minimum requirements, certifications and audits supported), risk management (e.g. dissemination of knowledge and use of best practices), liabilities (e.g. defined liability, dispute resolution) and compliance (e.g. general compliance, privacy issues).”

Circle of Trust One or more service providers and identity providers that have business relationships and operational agreements, and with whom users can transact business in a secure and apparently seamless environment.

Data Service Template See ID-WSF Data Service Template.

De-Federation A reversal of the process of Federation of two Accounts (belonging to the same Principal), or termination of the state of Identity Federation. De-Federation usually involves an exchange of messages among the systems which established the Identity Federation.

Discovery A mechanism that allows requestors to discover resources and how to access those resources.

Discovery Service See ID-WSF Discovery Service

End User An individual who uses services and content [OMADict]

Federation The binding of two or more Accounts (within an Authentication Domain or a Circle of Trust, where one of the Accounts is at an IDP) for a given Principal. Federation does not imply that Identity Attributes are being shared – it is simply a joining of two or more Accounts (e.g. for Single Sign On), after which Attributes could then be shared.

Entity Entity: 1 : The information transferred as the payload of a request or response. 2 : A distinct component of a service architecture [OMADict]. In this document the term Principal is regularly used as a subset of Entity, more specific to the Entities involved in an Identity Management enabler.

Identifier A reference that uniquely maps to an Identity. One or more Identifiers are among the characteristics that define an Identity.

Identity The characteristics by which an Entity or person is recognized or known.

Identity Federation Associating, connecting, or binding multiple Accounts for a given Principal at various entities within a Circle of Trust. (Source: [Liberty-Glossary])

Identity Provider A special type of Service Provider role that creates, maintains, and manages Identity information for Principals, and can provide an Authentication Assertion to other Service Providers within an Authentication Domain (or even a Circle of Trust).

ID-WSF Authentication Service The ID-WSF Authentication Service is a Liberty Alliance specification that allows generic identity authentication information exchange over SOAP in order to implement a WSC/WSP peer to peer authentication.

ID-WSF Enabled Web Service Provider A Web Service provider that supports the Liberty ID-WSF protocols as specified in this specification.

ID-WSF Data Service Template The ID-WSF Data Service Template is a Liberty Alliance specification that defines common data access protocols to allow querying and modifying arbitrary data items according to the application (e.g. an application may simply use or extend the DST protocol to provide a basic query/modify interface to application clients without having to design or code such functionality itself).

ID-WSF Discovery Service The ID-WSF Discovery Service is a Liberty Alliance specification that enables various entities (e.g. service providers) to dynamically discover a principal's registered services. Given the type of service desired, the Discovery Service responds with a service description containing WSDL for the desired identity service, provided that permissions set by the Principal allow the disclosure of these resources to the relevant entity. The Discovery Service can also function as a security token service, issuing security tokens to the requester that the requester will use in the request to the discovered identity service.

ID-WSF Interaction Service The ID-WSF Interaction Service is a Liberty Alliance specification that allows an identity service to interact with the owner of a requested resource that it is exposing, in order to collect attribute values, or to obtain permission to share the data with a Web Services Consumer.

ID-WSF Security Mechanisms The ID-WSF Security Mechanisms is a Liberty Alliance specification that describes profiles and requirements for securing the discovery and use of web services. It includes security requirements to both protect privacy, and to ensure integrity and confidentiality of messages between service providers.

ID-WSF SOAP Binding The ID-WSF SOAP Binding Mechanisms is a Liberty Alliance specification that provides a SOAP-based invocation framework for identity services. This binding does not specify any contents for the SOAP body itself, but offers an extensibility model by defining headers addressing message exchange specifics (i.e. consent claims, affiliation declaration, etc)

Interaction Service See ID-WSF Interaction Service.

LUAD User agents and devices that send or consume protocol messages specified in the Liberty Alliance ID-WSF (or ID-FF) specifications are called *Liberty enabled User Agents and Devices*. The defining characteristic of a LUAD is that it is closely associated with one user (or a few users, such as a family).

LUAD-WSC A LUAD that is invoking services provided by an ID-WSF Enabled Web Service Provider

LUAD-WSP A LUAD that is acting as an ID-WSF Enabled Web Service Provider

Network Identity The abstraction of the global set of attributes composed from all of a Principal's existing Accounts

PAOS A reversed HTTP binding for SOAP wherein a SOAP request is attached to an HTTP response. Examples of scenarios where the reversed HTTP binding for SOAP may be used are:

A provider is hosted on a device that supports a HTTP client but not a HTTP server. This may be the case when the device is resource constrained.

A provider is hosted on a device that is not generally addressable or reachable from the Internet

Principal An entity that has an identity, that is capable of providing consent and other data, and to which authenticated actions are done on its behalf. Examples of principals include an individual end user, a group of end users, a corporation, service enablers / applications, system entities and other legal entities. [OMADict]

Proxy A computer process that relays a protocol between client and server computer systems, by appearing to the client to be the server and appearing to the server to be the client. (Source: [RFC 2828])

Pseudonym An arbitrary name assigned by the Identity Provider or Service Provider to identify a Principal to a given relying party, so that the name has meaning only in the context of the relationship between the relying parties.

Resource Offering A resource offering is the association of a resource and a service instance. This association is necessary as there is a many-to-many relationship between resources and service instances. A single service instance may serve many resources. For example, a personal profile service provider would typically serve up many profiles behind a single service instance, as having a separate protocol endpoint for each profile would be impractical. [Liberty-idwsf-disco].

Security Mechanisms See ID-WSF Security Mechanisms.

Service Instance A service instance is a running Web Service at a distinct protocol endpoint [Liberty-idwsf-disco].

Service Provider An Entity that provides services and/or goods to Principals.

Single Log Out The ability for End Users to properly terminate all open connections, active services or relationships associated with a Single Sign On (SSO) Session, with one logout process.

Single Sign On The ability to use an Authentication Assertion from one Provider (an Identity Provider or an Identity Broker) at another Provider, in order to ease the burden (for a Principal) of having to authenticate to each Provider separately within a single Session.

SOAP Binding See ID-WSF SOAP Binding.

Subscriber A Subscriber is an entity (associated with one or more users) that is engaged in a Subscription with a Service Provider. The subscriber is allowed to subscribe and unsubscribe services, to register a user or a list of users authorised to enjoy these services, and also to set the limits relative to the use that associated users make of these services. (Source: [3GPP-TR21.905])

Subscription A subscription describes the commercial relationship between the Subscriber and the Service Provider. (Source: [3GPP-TR21.905])

Trust The extent to which someone that relies on a system can have confidence that the system meets its specifications, i.e., that the system does what it claims to do and does not perform unwanted functions. [source:RFC2828]

WS-Security WS-Security describes enhancements to SOAP messaging to provide *quality of protection* through message integrity, message confidentiality, and single message authentication. These mechanisms can be used to accommodate a wide variety of security models and encryption technologies.

User Agent Any software or device that acts on behalf of a user, interacting with other entities and processing resources. (Source: [OMADictionary-v1.0])

3.3 Abbreviations

ERDEF	Enabler Requirement Definition
ERELD	Enabler Release Definition
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP Secure (aka HTTP over SSL)
LECP	Liberty Enabled Client/Proxy
MIME	Multipurpose Internet Mail Extensions
OASIS	Organization for the Advancement of Structured Information Standards
OMA	Open Mobile Alliance
OWSER NI	OMA Web Services Network Identity Enabler
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol (no longer an acyronym starting with SOAP version 1.2)
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDDI	Universal Description, Discovery and Integration
URI	Uniform Resource Identifier
WS	Web Services
WSDL	Web Services Definition Language

4. Introduction

This document outlines the Enabler Release Definition for the OMA Network Identity Web Services Enabler (OWSER NI).

The OWSER NI Version 1.0 consists of two specifications:

- The “OMA Web Services Network Identity Enabler (OWSER NI): Identity Federation Framework “[OWSER NI FF] provides the protocols and services to enable federated identity in a Liberty-enabled Web services environment.
- The “OMA Web Services Network Identity Enabler (OWSER NI): Identity Web Services Framework” [OWSER NI WSF] provides the specifications of the components needed to to support Web Services based access to, and sharing of, attributes related to a Principal in a privacy-protected manner in a Liberty-enabled Web services environment .

The OWSER NI specifications are augmented by an informative Architecture Document [OWSER NI AD] document that provides additional information to readers of the specifications:

It is important to note that there are no implications that other OMA enablers are required to provide their functionality via OWSER Network Identity. However, for those enablers that choose to do so, the corresponding OWSER NI specifications provide normative guidance. Without such normative guidance, designers of Identity Web Services within OMA would solve these problems on their own, each in their own way. This would lead to interoperability problems and increased time to market.

Implementers should make themselves familiar with the Liberty Alliance Identity Federation Version 1.1 and Liberty Alliance Identity Web Services Framework version 1.1 specifications [LAP] as these are referenced heavily in the [OWSER NI] as the external specifications with which OMA enablers using Liberty technologies to offer the above-mentioned network identity features should be conformant

5. OWSER NI Enabler Release Specification Baseline

The following specifications comprise the OWSER Network Identity Enabler

Doc Ref	Permanent Document Reference	Description
Requirement Document		
[NI REQ]	OMA-RD-OWSER-NI-V1_1-20051220-C.	Requirement Document for OWSER NI Enabler
Architecture Document		
[OWSER NI AD]	OMA-AD-OWSER_NI-V1_0-20051220-C	Architecture Document for OWSER NI Enabler
Technical Specifications		
[OWSER NI FF]	OMA-TS-OWSER_NI_FF-V1_0-20051220-C	Federation Framework specification for OWSER NI Enabler
[OWSER NI WSF]	OMA-TS-OWSER_NI_WSF-V1_0-20051220-C	Web Service Framework specification for OWSER NI Enabler

6. Minimum Functionality Description for OWSER NI

6.1 Identity Federation Framework (ID-FF)

An OMA Service Enabler offering Identity Federation features defined in [OWSER NI FF] must support, as appropriate, the roles of a LECP, an Identity Provider, or a Liberty Enabled Service Provider in offering the following mandatory features:

- Single sign on and federation
- Single sign out
- Federation termination
- Affliliations
- Dynamic proxying of Identity Providers

Optional features include support of a HTTP POST end user agent and Name Registration and Authentication Context interactions between an Identity Provider and a Service Provider. If supported, implementations of these features must conform to that described in [OWSER NI FF].

When transport and message level security are required in interactions between a LECP, Identity Provider and a Service Provider, the use of the corresponding techniques in [OWSER SPEC] are mandated.

6.2 Identity Web Services Framework

An OMA Service Enabler offering Identity Web Service Framework features defined in [OWSER NI FF] must support, as appropriate, the roles of an Identity Provider, a Liberty Discovery Service, , a Liberty Interaction Service, a Liberty Enbaled Service Provider, or a Liberty Enabled User Agent or Device (LUAD-WSP, LUAD-WSC) in offering the following mandatory features:

- ID-WSF Bootstrap
- Discovery Lookup
- Discovery Update
- Interaction redirect
- Authentication

Optional features include Authorization, use of the Liberty Data Services template by Attribute Providers to implement Attribute Query/Lookup, use of the PAOS binding, and Usage Directives. If supported, implementations of these features must conform to that described in [OWSER NI WSF].

7. Conformance Requirements Notation Details

This section is informative

The tables in following chapters use the following notation:

Item: Entry in this column MUST be a valid ScrItem according to [IOPPROC].

Feature/Application: Entry in this column SHOULD be a short descriptive label to the **Item** in question.

Status: Entry in this column MUST accurately reflect the architectural status of the **Item** in question.

- M means the **Item** is mandatory for the class
- O means the **Item** is optional for the class
- NA means the **Item** is not applicable for the class

Requirement: Expression in the column MUST be a valid TerminalExpression according to [IOPPROC] and it MUST accurately reflect the architectural requirement of the **Item** in question.

8. ERDEF for OWSER NI

This section is normative.

Item	Feature / Application	Status	Requirement
Item	Feature / Application	Status	Requirement
OMA-ERDEF-OWSER-NI-000	Identity Federation Framework, Identity Web Services Framework	M	OMA-ERDEF-OWSER-NI-FF-000 OR OMA-ERDEF-OWSER-NI-WSF-000

Note that the entries in the requirements cells make references to Item entries in sections 8.1 and 8.2

Table 1 ERDEF for OWSER NI

8.1 Identity Federation Framework Requirements

An enabler that references the Identity Federation Framework functionality described in [OWSER NI FF] MUST conform to that specification.

Expressions in the Requirements column in the tables below reference Items in Appendix A of [OWSER NI FF].

In the Requirements columns in the tables below, the following terms are used:

- MIDFFF: mandatory features for Identity Federation Framework

Item	Feature / Application	Status	Requirement
OMA-ERDEF-OWSER-NI-FF-000	Network Identity Federation Framwork	O	MIDFFF

Table 2 ERDEF for OWSER NI Identity Federation Framework

8.2 Identity Web Services Framework (WSF) Requirements

An enabler that references the Identity Web Services Framework functionality described in [OWSER NI WSF] MUST conform to that specification.

Expressions in the Requirements column in the tables below reference Items in Appendix A of [OWSER NI WSF].

In the Requirements columns in the tables below, the following terms are used:

- MIDWSFF: mandatory features for the Identity Web Services Framework

Table 3 ERDEF for OWSER NI Identity Web Services Framework

Item	Feature / Application	Status	Requirement

OMA-ERDEF-OWSER-NI-WSF-000	Network Identity Web Services Framework	O	MIDWSFF

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Version	09 Oct 2003		Prepared for Consistency Review.
OMA-ERELD-OWSER-NI-V1_0-20051205-D	05 Dec 2005	2,5	Fixed references to files in package.
Candidate Version OMA-ERELD-OWSER_NI-V1_0	20 Dec 2005		Status changed to Candidate by TP TP ref # OMA-TP-2005-0396-OWSER_NI_V1_0_for_Candidate_approval