Liberty Content SMS and MMS Specification

Version: 1.0

Editors:
Sampo Kellomäki, Symlabs, Inc.

Contributors:
Robert Aarts, Hewlett-Packard
Maria Carmen Aparicio, Telefónica Móviles
Carolina Canales Valenzuela, Ericsson
Peter Davis, NeuStar
Rob Lockhart, IEEE-ISTO
Guillermo Lorenzo, Symlabs, Inc.
Antonio Navarro, Symlabs, Inc.
Susana Ochoa, Vodafone
David Perez, Telefónica Móviles
David del Ser, Vodafone

Abstract:
The Liberty Content SMS and MMS Specification (ID-SIS-CSM) layers on MM7 to add identity-based invocation and addressing. It leverages the Liberty ID Web Services Framework (ID-WSF) to do this. It enables Principals wielding Liberty identities to access Value Added Services (VAS), such that privacy is preserved and mobile spam is controlled, while allowing the Value Added Service Providers (VASPs) to offer more personalized service using controlled sharing of user and device attributes. The user is identified independently of delivery channel and, indeed, multiple channels can be supported.

The ID-SIS-CSM consists of Mobile Originated (MO) and Mobile Terminated (MT) interfaces that are quite independent, but can be combined to form round trip scenarios. The MO interface allows a mobile Principal to invoke, by sending a message, a VAS using Liberty Single Sign On (SSO) such that the VASP has assurance of the Principal’s identity and is able to further invoke ID Web Services on behalf of the Principal. The MT interface allows a VASP that has obtained a Principal’s discovery or MT resource offering to send messages and content to the Principal by invoking the MT ID Web Service.

Filename: liberty-id-sis-csm-v1.0.pdf
Notice

This document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby granted to use the
document solely for the purpose of implementing the Specification. No rights are granted to prepare derivative works
of this Specification. Entities seeking permission to reproduce portions of this document for other uses must contact
the Liberty Alliance to determine whether an appropriate license for such use is available.

Implementation of certain elements of this document may require licenses under third party intellectual property
rights, including without limitation, patent rights. The Sponsors of and any other contributors to the Specification are
not and shall not be held responsible in any manner for identifying or failing to identify any or all such third party
intellectual property rights. This Specification is provided "AS IS," and no participant in the Liberty Alliance
makes any warranty of any kind, express or implied, including any implied warranties of merchantability,
non-infringement of third party intellectual property rights, and fitness for a particular purpose. Implementers
of this Specification are advised to review the Liberty Alliance Project’s website (http://www.projectliberty.org/) for
information concerning any Necessary Claims Disclosure Notices that have been received by the Liberty Alliance
Management Board.

Copyright © 2005-2007 Ericsson; Hewlett-Packard Development Company, L.P.; NeuStar, Inc.; Sun Microsystems,
Inc.; Symlabs, Inc.; Telefónica Móviles; and Vodafone Group Plc. All rights reserved.

Liberty Alliance Project
Licensing Administrator
c/o IEEE-ISTO
445 Hoes Lane
Piscataway, NJ 08855-1331, USA
info@projectliberty.org
Contents

1. Introduction .......................................................... 4
  1.1. Motivation ......................................................... 4
  1.2. Mobile Originated (MO) Scenario and Roles .................. 4
  1.3. Mobile Terminated (MT) Scenario and Roles ................ 6
  1.4. Combined MO and MT Scenario ................................ 7
  1.5. Combined MT and MO Scenario ................................ 7
  1.6. Notational Conventions ....................................... 7
  1.7. Derivation of ID-SIS-CSM from MM7, ID-FF, SAML 2.0, and ID-WSF ................................................. 8
  1.8. Compliance ..................................................... 8
  1.9. Namespaces .................................................... 9

2. MO Service ............................................................. 10
  2.1. MO5 Message .................................................... 10
  2.2. MO6 Message .................................................... 10
  2.3. Other MO Processing Rules ................................... 10
  2.4. MO ECP Profile ................................................. 10
  2.5. MO LECP Profile .............................................. 10
  2.6. MO ID-WSF 1.1 SSOS Profile ................................ 11

3. MT Service ............................................................. 12
  3.1. MT3 Message and Its Response ................................ 12
  3.2. MT7 Message and Its Response ................................ 12
  3.3. MT ID-WSF 1.1 Profile ....................................... 12

4. Protocol Features .................................................... 13
  4.1. Discovery Registrations ....................................... 13
    4.1.1. Discovery Options to Indicate Supported MM7 Versions 13
    4.1.2. Implementation-Dependent Discovery Options .......... 13
  4.2. Addressing One Message to Multiple Recipients ............ 13
    4.2.1. Using Liberty ID-WSF 1.1 ResourceID for Addressing 13
  4.3. Mixing Frameworks ............................................ 14
  4.4. Securing Attached Message Contents ....................... 14

5. Guidance ............................................................... 16
  5.1. VASP Aggregation .............................................. 16
  5.2. Accounting and Customer Care ................................. 16

6. Using ID-SIS-CSM with MM7 XML Schema ........................ 17

7. Examples .............................................................. 18
  7.1. MO Round Trip ................................................. 18
  7.2. MT Round Trip ................................................. 24
  7.3. MT to Multiple Recipients ................................... 27

8. Annex: Legacy Messaging Features ................................. 31
  8.1. Representation of Content ................................... 31
  8.2. SMS Support .................................................. 31
  8.3. Indication of Sending Preferences for MT .................... 32
  8.4. Support for WAP Push ......................................... 32
  8.5. MMStatus Indications Regarding State of the Message .... 33
  8.6. Querying State of MT messages ............................... 33
  8.7. Additional Schema to Support Legacy Messaging ............ 33

References ............................................................. 35
1. Introduction

MM7 [MM7] is an industry standard for mobile messaging that has enjoyed success especially in MMS content and messaging, yet it is generic enough to be used for other messaging technologies like SMS and can be easily translated to other protocols such as SMPP. MM7 is a regular Web Service that is based on SOAP 1.1 with attachments [SOAPattach] and with MIME multipart content [RFC2387].

Liberty ID Web Services Framework (ID-WSF) is an enabling technology that allows identity-based access and addressing to be added to existing web services, such as MM7. ID-WSF adds certain elements to convey the identity information, such as SAML assertions, and requires little or no alteration to the SOAP body. It allows an existing Web Service to be leveraged to create a new ID-enabled web service. The objective of this document is to describe just such a protocol and service: the ID-SIS-CSM.

ID-SIS-CSM is an identity service because (i) messages are addressed to an identifiable Principal, (ii) the Principal's consent to receive messages from a VASP is conveyed using robust Liberty ID-WSF mechanisms that prevent the VASPs from forging the consent, and (iii) the ID-WSF mechanisms also enable better privacy.

Scope: This specification specifies identity web services interfaces between an identity messaging server (MO and MT roles, defined later), an IdP, and a VASP.

Out of scope: This specification does NOT specify interfaces between an identity messaging server and rest of the messaging system. Any references to MM7 and MMSC are for illustration, only. Non-messaging identity web services are out of scope as well, but they are defined in other Liberty Alliance specifications.

1.1. Motivation

Many popular Value Added Service Providers (VASP) deliver content to the mobile phones of their users. In some cases, mobile content delivery is the primary service offered, for example, services that offer ring tones or phone logos and screen savers. In other cases, mobile messaging is used by a VASP to enhance its other services, for example, airlines offer to send short messages about flight status. In order for a VASP to send messages to a mobile phone of a user, it needs both access to a delivery system as well as the mobile phone number of the user. In many cases, however, the nature of the service does not justify the privacy hazard that occurs when the user has to give her mobile phone number. This specification aims to overcome this problem by suggesting the use of the Liberty ID-WSF specifications to exchange pseudonymous or anonymous identifiers for the users between the VASP and the delivery system.

Many of the aforementioned service providers offer their services through a Short Message Service (SMS) interface. That is, end users can request some service, information, or content by sending a short message from their phone to a well-known short number. Typically, the short number identifies the service provider and the message structure is rigorously defined to carry the necessary request information. For example, a user may obtain a ring tone by sending "RING Feel" to 12345. Typically, users find these services and instructions through advertisements. To reply with the content, the VASP again needs the mobile phone number of the user. It is important to note that the same user may at other times access the VASP through a normal browser session. It would be advantageous if the VASP would have the possibility to recognize the user independently from the service access channel, browser, or messaging.

For all VASPs, it is beneficial to provide highly personalized content. This is especially true for the SMS-based services described above, as the user interface in this case is very poor. Consider a horoscope service. For example, to offer a proper service, it would need the birthday of the user, but typing something like "HS 15.4.1972" is much more cumbersome than simply "HS." The ID-WSF framework allows for VASPs to discover and use identity services for the user, e.g., for personal profile information, geolocation, etc.

1.2. Mobile Originated (MO) Scenario and Roles
In the MO scenario, a principal sends a message (MO1) to a number, usually a short code. The message is processed by a messaging server, such as an MMSC. The messaging server understands, perhaps from the short code, that the message should be forwarded (MO2, e.g., DeliverReq) to the MO-Relay. Everything up to this point is in the Mobile Messaging Domain and out of scope for this specification. Suffice to say that mechanisms like MM7 or SMPP may be used on interface (MO2).

Upon receiving the message, MO-Relay proceeds to perform Single Sign On using an IdP. This involves sending an AuthnFed request (MO3) using one of the protocols profiled later, e.g., LECP, ECP, or SSOS.

The IdP uses a mobile authentication method to authenticate the Principal. Exactly how this happens is not within the scope of this specification, but perhaps a trusted MSISDN HTTP header was passed to convey the SIM card-based network layer authentication. This would assume that the IdP can trust the MO-Relay - most probably they would be in same trusted network and operated by the same business entity.

The IdP generates a SAML assertion with AuthnStmt containing the Principal’s pseudonymous NameID, to be consumed by the ID-VASP, and AttributeStmt, containing ID-WSF Discovery Bootstrap that allows ID Web Services to be invoked. The assertion is sent (MO4) to the MO-Relay, which forwards it (MO5, <DeliverReq> + <AuthnResp>) to the ID-VASP. This is effectively an unsolicited authentication response. It knows to which ID-VASP to send the message by mapping the number or short code to the ID-VASP’s end point URL for MO interface. Presumably, there is some routing table or other implementation-dependent means for determining this. All of this happens using one of the protocols profiled later in this document, e.g., LECP, ECP, or SSOS.

Now, the ID-VASP consumes the assertion, notices that the user is valid, and interprets the service request. The ID-VASP may perform any desired processing, but finally it has to reply (MO6, <DeliverRsp>) to the MO-Relay, confirming that the message, sent by the user, was correctly received. Upon (MO6), the MO-Relay may acknowledge the message to the messaging server (e.g., <DeliverRsp> to MMSC) which may take any appropriate and necessary action in the mobile network.

If the VAS involves a reply with content, the MT scenario will be used to send this reply. While the ID-VASP will not know the Principal’s phone number, it will have the means to make an ID Web Service call that conveys enough information for the MT-Relay to figure out the phone number and other parameters needed to send the content to the Principal. At any rate, the content will be sent asynchronously with respect to message (MO6).

In processing the message (MO5, <DeliverReq>), the ID-VASP may invoke ID Web Services. Typically, it would invoke (MO5.1) the Discovery Service to find out the end point for the ID Web Service of interest and then call (MO5.2) the ID-WSP to obtain some service, or perhaps attributes about the Principal or her handset. All these interactions are enabled by the present specification, but use regular ID-WSF mechanisms and are therefore not in the scope of this specification.

Roles defined
ID-SIS-CSM MO-Relay  
This entity acts as LECP, ECP, or SSOS WSC in order to effectuate SSO and to pass the message to the ID-VASP. It will also have to talk some messaging protocol, such as MM7 or SMPP towards the Mobile Messaging Domain. How this happens is not within the scope of this specification. The MO-Relay is a functional entity acting on behalf of the user in the Liberty-based interactions. The concrete realization of this entity is not within the scope of this document, e.g., MO-Relay may be one or several logical elements at the whim of the implementer.

IdP  
There is nothing special about this entity other than that it must accept mobile authentication. How it does this is not within the scope of this specification. Any Liberty ID-FF 1.2-, ID-WSF 1.1-, or SAML 2.0-certified IdP can be used. As IdPs are well-specified in other specifications, they will not be further described in this specification.

ID-VASP  
This is a special type of VASP that speaks the protocol described in this specification (steps 5 and 6). An ID-VASP may also make ID-WSF Web Service calls such as calling the ID-SIS-CSM MT service to send content requested by the Principal. The latter aspect employs normal mechanisms documented in Liberty ID-WSF specifications and will not be discussed further in this specification.

1.3. Mobile Terminated (MT) Scenario and Roles

Figure 2. MT Scenario and Roles

In the MT scenario, the Principal performs a Single Sign On (SSO) (MT1) using some federated identity protocol with which we do not have to concern ourselves except to the extent that the VASP, which acts as an ID-SIS-CSM WSC, will receive a discovery bootstrap containing a resource offering (RO) for the discovery service. The SSO operation could be the MO scenario, above, or it could be something else, perhaps a LUAD or web-based SSO. The RO may also have been received earlier by other means, such as a previously created subscription.

The ID-SIS-CSM WSC discovers (MT2) the ID-SIS-CSM MT-Relay using the discovery service indicated by the RO in the bootstrap. As a precondition for this to succeed, the ID-SIS-CSM MT-Relay must have been registered for the Principal. This registration may have happened by a request of the Principal, previously, and using standard ID-WSF protocols, or it could have happened using some implementation-dependent, out-of-band method, such as a default value or bulk registration. All this is standard ID-WSF usage and will not be discussed further within this document.

The ID-SIS-CSM WSC contacts (MT3, e.g., <SubmitReq>) the ID-SIS-CSM MT-Relay using the ID-WSF-based protocol described in this document. The ID-SIS-CSM MT-Relay contacts (MT4, e.g., <SubmitReq>) the messaging server (e.g., MMSC) or other Mobile Messaging Domain entity to request delivery (MT5) of the message. In reply to (MT4, e.g., <SubmitRsp>), the ID-SIS-CSM MT-Relay will get confirmation about acceptance of the message for delivery which it passes (MT3) back to ID-SIS-CSM WSC.

If the ID-SIS-CSM WSC requested a delivery receipt, this will be sent asynchronously. Generally, the messaging server will send (MT6, <DeliveryReportReq>) the delivery receipt to ID-SIS-CSM MT-Relay in a way that is not within the scope of this specification and the MT-Relay will send (MT7) a notification to the ID-SIS-CSM WSC.

Liberty Alliance Project
Roles defined

ID-SIS-CSM MT-Relay  This entity acts as an ID Web Services Provider that sends mobile messages to the Principal. It has an ID-WSF-based interface, specified in the present document, and a Mobile Messaging Domain interface, perhaps MM7 or SMPP, that is not within the scope of this document.

The MT-Relay is a functional entity acting on behalf of the user in the Liberty-based interactions. The concrete realization of this entity is not within the scope of this document, e.g., the MT-Relay may be one or several logical elements at the whim of the implementer.

ID-SIS-CSM WSC  This is an ID-WSF-based ID Web Services Client that speaks the client half of the protocol described in this document. It usually also has some federation framework SP interface for SSO (MT1), but that interface is not within the scope of this document as long as it allows discovery or an ID-SIS-CSM MT service RO to be obtained.

Disco  This is a regular ID-WSF discovery service [LibertyDisco12]. While this entity is architecturally necessary, there is noting special about it. Any certified ID-WSF discovery service implementation can be used and thus will not be discussed further within this document.

1.4. Combined MO and MT Scenario

In this scenario, the Principal uses the MO to request some service which is then delivered using MT. It essentially combines MO and MT scenarios, but also creates the requirement that the ID-VASP has to be able to send a reply message using the WSP offered by ID-SIS-CSM MT-Relay. Since the MO scenario states that the ID-VASP must be able to call any ID Web Service, this requirement is trivially satisfied.

If the terminal or the MT-Relay needs to correlate the MT message to the MO message (i.e., MT is legitimate only if there was corresponding MO), it MAY use the <LinkedID> element, see [MM7], Section 8.7.1.3 "Features," p.109.

1.5. Combined MT and MO Scenario

In this scenario, the VASP, or any other entity that acts as an ID-SIS-CSM WSC, sends a message, using the MT scenario, to the Principal, requesting a reply. If the Principal replies, the MO scenario is used to deliver the reply to the VASP, which, in this case, acts in the ID-VASP role.

This scenario generates two special requirements.

1. The message sent in MT must be replyable, e.g., perhaps it appears to have been sent from the short code of the ID-VASP.

2. It must be possible to correlate the MO message to the MT message. This can be accomplished either
   a. by the content of the reply, e.g., the reply must contain the code that was sent in the MT message, or
   b. by using some messaging level correlation mechanism.
Obviously, there are certain dangers in sending messages to the Principal and asking her to reply to them. A sensible protection against these threats is to limit in the MT-Relay or the Mobile Messaging Domain, e.g., in the MMSC, the possible "From" addresses that a given ID-SIS-CSM WSC can spoof.

1.6. Notational Conventions

This document is a Liberty ID Web Services Interface Specification that normatively specifies the ID-SIS-CSM Service.

In case of disagreement between the present document and any guidelines or XML schema descriptions, this document is prescriptive. Any published errata is hereby incorporated to this document by reference and as such is normative.

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

N.B. [MM7] and colloquial messaging terminology is used where ever possible even when Liberty terminology collides.

1.7. Derivation of ID-SIS-CSM from MM7, ID-FF, SAML 2.0, and ID-WSF

The ID-SIS-CSM MO service is formed by extending Liberty ID-FF 1.2 LECP [LibertyBindProf], Section 3.2.4 "Liberty-Enabled Client and Proxy Profile," or SAML 2.0 ECP [SAMLProf2], Section 4.2 "Enhanced Client or Proxy (ECP) Profile," by adding an MM7 [MM7] payload to the message (MO5, <DeliverReq> + <AuthnResp>), or by employing regular Liberty ID-WSF Single Sign-On Service [LibertyAuthn11], to obtain an assertion which is then added to the MM7 payload of message (MO5). All stipulations of these specifications are incorporated, unless expressly waived in this specification.

Different federation framework versions (i.e., LECP vs. ECP vs. SSOS) are accommodated by separate profiles that appear as part of this specification. All implementations MUST implement the ECP-based profile while the LECP and SSOS-based profiles are OPTIONAL. An implementation SHOULD state which versions it supports.

The ID-SIS-CSM MT service is formed from MM7 [MM7] by adding ID-WSF 1.1 [LibertySOAPBinding12]-specified SOAP headers to convey the identity of the Principal and addressing. All stipulations of these specifications are incorporated, unless expressly waived in this specification.

Both MO and MT services can be implemented using various versions and sub-versions of the MM7 specification. All implementations MUST support [MM7] (the specific version) and MAY support other versions. An implementation SHOULD state which versions it supports. Note that this restriction does not apply to the MO2 and MT4 interfaces.

1.8. Compliance

This specification defines an interface to which an implementation and an instance (deployment, ID-VASP) of ID-SIS-CSM service MUST conform. For an ID-VASP to be ID-SIS-CSM compliant, it MUST adhere to all aspects of the specification.

A minimally-compliant ID-SIS-CSM implementation MAY choose not to support optional features of this specification. Such an implementation may be labeled as an "ID-SIS-CSM implementation" provided that publicly available documentation about the implementation clearly discloses which optional parts of the schema and which features are not supported. All other features and schema are assumed to be supported. A deployment of an implementation that is not capable of supporting the full schema SHOULD only register the discovery option keywords that accurately reflect its capabilities.
An implementation that only supports Mobile-Originated operation is termed an "ID-SIS-CSM MO implementation."
Within the MO scenario, the ID-SIS-CSM MO-Relay and ID-VASP roles exist. If an implementation only supports
one of the roles, its labeling MUST indicate which.

An implementation that only supports Mobile-Terminated operation is termed an "ID-SIS-CSM MT implementation."
Within the MT scenario, the ID-SIS-CSM MT-Relay and ID-SIS-CSM WSC roles exist. If an implementation only
supports one of the roles, its labeling MUST indicate which.

An implementation that supports all of the schema and features specified in this document, including Annex, in all roles
MAY be labeled as a "full ID-SIS-CSM implementation." An implementation that falls short on any feature or part of
the schema MUST NOT be labeled as a "full ID-SIS-CSM implementation." A "full ID-SIS-CSM implementation"
deployment MAY administratively, or via configuration, restrict the schema and features.

An ID-SIS-CSM implementation MUST publicly disclose which federation framework, ID-WSF, and MM7 versions
it supports. Labeling of an implementation that does not yet support SAML 2.0 must be qualified by the designator
"(interim)."

A deployment that supports all of the schema and features specified in this document MAY be labeled as a "full
ID-SIS-CSM deployment" or a "full ID-SIS-CSM service." To meet full ID-SIS-CSM deployment status, all of the
schema and features MUST be supported for all Principals wishing to use them, barring a policy decision excluding
some Principal.

A deployment that only supports some subset of ID-SIS-CSM may still be labeled as an "ID-SIS-CSM deployment"
or an "ID-SIS-CSM service" provided that the deployment publicly discloses the subset that it supports.

An ID-SIS-CSM deployment or instance MUST publicly disclose which federation framework, ID-WSF, and MM7
versions it supports. Labeling of a deployment or implementation that does not yet support SAML 2.0 must be
qualified by designator "(interim)."

1.9. Namespaces

In the discovery registrations, the MT service is registered as service type

\texttt{urn:liberty:id-sis-csm:2006-02}

The addressing extensions, as well as legacy messaging extensions, described in the Annex are in their own namespace,
called "csm:" and denoted by the same URN as is used for service type. The extension points of MM7 addressing are
presumed to be defined in respective MM7 schema, here prefixed as "mm7:..

<table>
<thead>
<tr>
<th>Prefix</th>
<th>URI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mm7:</td>
<td>URI of chosen MM7 version</td>
<td>MM7 version, such as [MM7]. Some other specifications refer to this namespace as &quot;tns:&quot;</td>
</tr>
<tr>
<td>csm:</td>
<td>\texttt{urn:liberty:id-sis-csm:2006-02}</td>
<td>This service.</td>
</tr>
<tr>
<td>ds:</td>
<td>\texttt{urn:liberty:disco:2004-04}</td>
<td>Liberty ID-WSF Discovery Service \cite{LibertyDisco12}</td>
</tr>
<tr>
<td>xml:</td>
<td>\texttt{<a href="http://www.w3.org/TR/REC-xml%7D">http://www.w3.org/TR/REC-xml}</a></td>
<td>XML Definition [XML] (for xml:lang)</td>
</tr>
</tbody>
</table>
2. MO Service

2.1. MO5 Message

The MO5 message MUST be a valid MM7 message, including SOAP attachments and MIME multipart/related components, if needed. Typically, it is a <DeliverReq> message.

It may have been constructed by the MO-Relay or it may be passed almost directly from some source, such as MMSC or MO2 message (<DeliverReq>). Since MO2 generally is not signed, the MO-Relay has great license in sanitizing or re-crafting the message before it is passed on as MO5.

MO5 MUST NOT contain valid <Sender> information since this is conveyed by the single sign-on elements (e.g., SAML 2.0 <Response> or ID-FF 1.2 <AuthnResp>). If the message is being tunneled, the MO-Relay MUST sanitize this information away.

MO5 MUST contain, depending on profile, a <Response>, see [SAMLCore2] Section 3.3.3 "Element <Response>," or an <AuthnResponse>, see [LibertyProtSchema], element. This element MUST be passed in the SOAP <Body> right after the MM7 message (e.g., after <DeliverReq>) and MUST contain a SAML attribute statement describing a Discovery Bootstrap, see Section 6. "SAML AttributeDesignator for Discovery ResourceOffering" of [LibertyDisco12].

MO5 MUST contain HTTP and SOAP headers as mandated by profile, see below.

2.2. MO6 Message

The MO6 message MUST be a valid MM7 response, including SOAP attachments and MIME multipart/related components, if needed. This specification does not specify any extensions over MM7 for this message. Typically, it is a <DeliverRsp> message.

MO6 may be correlated to MO5 by virtue of the HTTP request - response mechanism. However, the ID-VASP SHOULD observe MM7 correlation requirements.

2.3. Other MO Processing Rules

If delivery receipt was requested at the MO2 interface, the MO-Relay SHOULD generate it upon receiving MO6.

2.4. MO ECP Profile

The MO-Relay MUST act in Enhanced Client role and the ID-VASP MUST act in SAML 2.0 SP role.

Normal ECP protocol MUST be implemented, as specified in [SAMLProf2], Section 4.2 "Enhanced Client or Proxy (ECP) Profile," with the following modifications:

a. The MO-Relay generates an unsigned <AuthnRequest> and sends (MO3) it to the IdP, i.e., the protocol starts at step 4, and

b. The message (MO5) in step 7 ("ECP Conveys <Response> to SP using PAOS") MUST have PAOS-related headers described in [SAMLProf2], Section 4.2.4.5 "PAOS Response Header Block: ECP to SP."
MO5 MUST have a `<Response>` element in its SOAP `<Body>`, as described above.

### 2.5. MO LECP Profile

The MO-Relay MUST act in LEC role and the ID-VASP MUST act in SP role.

Normal LECP protocol is implemented, as specified in [LibertyBindProf], Section 3.2.4 "Liberty-Enabled Client and Proxy Profile," with the following modifications:

a. The MO-Relay generates an unsigned `<AuthnRequest>` and sends (MO3) it to the IdP, i.e., the protocol starts at step 4, and

b. The message in step 7 ("Posting the Form Containing the `<AuthnResponse>`") MUST use MO5 format, described above. It MUST NOT be the LARES-based. MO5 MUST have the HTTP headers described in [LibertyBindProf], Section 3.2.4.1 "Liberty-Enabled Indications."

MO5 MUST have `<AuthnResponse>` element in its SOAP `<Body>`, as described above.

### 2.6. MO ID-WSF 1.1 SSOS Profile

The MO-Relay MUST act in LUAD role and the ID-VASP MUST act in SP role [LibertyAuthn11].

1. The MO-Relay invokes the AS in the normal fashion to authenticate itself and SSOS to obtain the discovery bootstrap.

2. The MO-Relay adds the `<AuthnResponse>` element from step 1 to the MO5 and sends it to the end point indicated by `AssertionConsumerServiceURL` meta-data element of the ID-VASP.

3. The ID-VASP replies with MO6.
3. MT Service

3.1. MT3 Message and Its Response

The MT3 message MUST be a valid MM7 message, including SOAP attachments and MIME multipart/related components, if needed.

The MT-Relay MUST look in the `<Recipients>` container and if it finds identity addressing tokens, see Section 4.2, convert them to messaging addresses as needed by backend technology. If it finds other addresses than identity addressing tokens, the behavior is implementation-dependent. The MT-Relay may, in this case, act as a regular MMSC or it may ignore such addresses or even flag an error.

MT3 MUST have SOAP headers prescribed by the profile, see below.

Response to MT3 MUST have SOAP headers prescribed by the profile, see below.

3.2. MT7 Message and Its Response

The MT7 message MUST be a valid MM7 message, including SOAP attachments and MIME multipart/related components, if needed.

It may have been constructed by MT-Relay or it may be passed almost directly from some source, such as MMSC or MT6 message. Since MT6 generally is not signed, MT-Relay has great license in sanitizing or re-crafting the message before it is passed on as MT7.

MT7 SHOULD NOT contain valid `<Sender>` information, unless it is not privacy sensitive, e.g., the Sender only identifies a well-known system entity such as the VASP. If the message is being tunneled, the MT-Relay MUST sanitize this information away.

MT7 is just a regular MM7 response. It does not have any ID-WSF properties. Determining the end point for sending an MT7 message is out of scope.

3.3. MT ID-WSF 1.1 Profile

MT3 is enhanced by adding the SOAP headers and signatures described in [LibertySOAPBinding12] and [Liberty-SecMech12] to it as is customary for ID-WSF 1.1-based services.

The MT-Relay creates a `<Recipients>` container, overwriting any previous `<Recipients>` container using the method described in Section 4.2

Once the `<Recipients>` has been constructed, the MT-Relay sends the message to the messaging server (e.g., MMSC) over the MT4 interface. The messaging server is expected to reply over this same interface with an MM7 response.

The MT-Relay sanitizes away from the MT4 response any identifiable information and uses it as the MT3 response.

The MT-Relay decorates the MT3 response with the SOAP headers and signatures described in [LibertySOAPBinding12] and [LibertySecMech12] as is customary for ID-WSF 1.1-based services.
4. Protocol Features

4.1. Discovery Registrations

Only the MT service needs to be registered in the discovery service with its service type. The MO "service" is not a service in an ID-WSF sense and, therefore, can not be registered.

The following discovery option keywords MAY be registered:

- urn:liberty:id-sis-csm:2006-02:deliveryreceipt: Delivery receipts are supported
- urn:liberty:id-sis-csm:2006-02:framework:sm: The MT service is SMS-capable
- urn:liberty:id-sis-csm:2006-02:framework:mm7: Regular, non-Liberty, MM7 is supported

4.1.1. Discovery Options to Indicate Supported MM7 Versions

An implementation MAY indicate its support for a specific version of the MM7 protocol by registering a discovery option of form

\[
\text{urn:liberty:id-sis-csm:2006-02:support:<mm7-ns-uri>}
\]

where the \(<mm7-ns-uri>\) is the namespace URI of the supported MM7 version. For example (very long so it may wrap out of right edge):

\[
\]

An implementation MAY register multiple such options to indicate support for multiple versions.

4.1.2. Implementation-Dependent Discovery Options

The implementers and deployers MAY define additional discovery option keywords to meet their special needs, provided that these keywords are properly qualified, e.g., using the domain name of the inventor to avoid conflicts. Such additional keywords MUST NOT start with urn:liberty. Some potential uses for additional keywords include advertising commercial properties such as cost or charging model so that a VASP can choose an appropriate gateway to use.

4.2. Addressing One Message to Multiple Recipients

An ID-SIS-CSM message may be addressed to any number of recipients, including one, identified by \text{identity addressing tokens}. The identity addressing token is an abstract notion that allows identity to be carried in the addressing field. Specific instances of the identity addressing token are defined in profiles, such as Section 4.2.1. A message may also be addressed to resolvable addresses, such as MSISDN or RFC822 addresses.

When an identity addressing token of some type is included in an MM7 \(<\text{To}>, \text{<Cc>}, \text{or <Bcc>}\) container, it conveys that the Principal has consented to receive messages from the sender as all Liberty-defined mechanisms require the user to be present, at some time in past no further than the validity period of the identity addressing token. In other words, for the VASP to have obtained the identity addressing token, the user must have performed a single sign-on somewhere and allowed the identity addressing token to be discovered or obtained.
The identity addressing token is carried in the MM7 message by placing it in the `<Extension>` element in an MM7 `<To>`, `<Cc>`, or `<Bcc>` container, see Section 6.

### 4.2.1. Using Liberty ID-WSF 1.1 ResourceID for Addressing

When using Liberty ID-WSF 1.1, the addressing information is expressed by a `<ResourceID>` or an `<EncryptedResourceID>` element. To bind the addressing to credentials, an `<IdentityAddressingToken>` container is introduced such that it contains both `<ResourceID>` or `<EncryptedResourceID>` and `<CredentialRef>` elements. The latter is used to reference a SAML assertion that serves as a credential. The `<IdentityAddressingToken>` acts as identity addressing token in the sense of Section 4.2.

#### Schema

```xml
<xs:element name="IdentityAddressingToken"
    type="csm:IdentityAddressingTokenType"/>
<xs:complexType name="IdentityAddressingTokenType">
    <xs:sequence>
        <xs:group ref="ds:ResourceIDGroup" minOccurs="1" maxOccurs="1"/>
        <xs:element name="CredentialRef" type="xs:IDREF"
            minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
</xs:complexType>
```

The `ResourceIDGroup` expresses either a `<ResourceID>` or an `<EncryptedResourceID>`. There MUST be exactly either one or another. An `<IdentityAddressingToken>` can address only one Principal. Use multiple tokens for addressing multiple Principals.

N.B. Addressing a single Principal works using this same mechanism: just supply only one `<IdentityAddressingToken>`. This approach is somewhat different that in some other ID-WSF-based services where the credentials in the SOAP header implicitly specify the targeted Principal. With the `<IdentityAddressingToken>`, the credentials in the SOAP header can still affect determination of the Principal because they can be referenced using `<CredentialRef>`.

 `<CredentialRef>` contains a "pointer" to the credential assertion, typically carried somewhere in SOAP headers. The contents of the `<CredentialRef>` element MUST match the ID XML attribute of the corresponding SAML assertion. `<CredentialRef>` SHOULD be used, but there may be special scenarios, e.g., in a trusted network, where it can be dispensed.

#### Example

```xml
<Assertion ID="CREDI-1234156154574djask"> ... </Assertion>
...<IdentityAddressingToken>
<ResourceID>http://mt-gw.com/4m082k15csaUxs</ResourceID>
<CredentialRef>CREDI-1234156154574djask</CredentialRef>
</IdentityAddressingToken>
```

The MT-Relay is responsible for performing discovery registrations such that Principals using the same MT-Relay can indeed be identified as such by the ID-SIS-CSM WSC. It is RECOMMENDED that the MT-Relay uses the same end point and security mechanism for all Principals. If different end points are used, the ID-SIS-CSM WSC may be lead to believe that they point to different MT-Relays and, thus, can not be batched.

### 4.3. Mixing Frameworks
ID-SIS-CSM is designed such that the choice of Single Sign-On framework (a.k.a. Federation Framework) is independent of the Identity Web Services Framework and vice versa. Thus, it is possible to use SAML 2.0 SSO and ID-WSF 1.1 together. See [LibertyCrossFramework] for guidance.

4.4. Securing Attached Message Contents

Following MM7, the ID-SIS-CSM allows message contents to be carried partially or entirely as MIME attachments [SOAPattach]. When such attachments are used, they MAY be secured as described in [wss-swa]. The message payload MAY use its own security mechanism. Such security mechanisms are outside the scope of this document.
5. Guidance

5.1. VASP Aggregation

As content messaging is an existing industry with value chains and solutions in place, it is desirable to keep them as much as they are. One particular player that has emerged is a VASP Aggregator.

A VASP Aggregator interacts with one or multiple mobile operators on behalf of a large number of VASPs. This allows mobile operators to maintain only few contact points to the vast number of VASPs out there.

ID-SIS-CSM supports the VASP aggregator model and, indeed, a VASP Aggregator can add a lot of value to its VASPs by interfacing ID-SIS-CSM to legacy protocols that are already used in industry and by acting as systems integrator.

There are two basic cases of VASP aggregation that need to be handled differently under ID-SIS-CSM due to the ability to reply and to privacy requirements.

1. Aggregation of many simple VASPs
   - aggregator acts as ID-VASP,
   - VASPs may continue to talk old protocols (aggregator translates), and
   - Use temporary NameIDs to preserve privacy and avoid collusion (same NameID towards all aggregated VASPs, but different ID is used every time).

2. Aggregation of VASPs that need to remember state about users
   - must use persistent NameID,
   - every aggregated VASP must have a different persistent NameID in order to avoid collusion,
   - this means that we need a separate ID-VASP for every underlying VASP,
   - aggregator operates a farm of virtual ID-VASPs, one per short code, and
   - as long as virtualization can be managed efficiently, aggregator’s business will be good and add value to VASPs.

5.2. Accounting and Customer Care

A real life problem that is common in the content messaging industry is that users repudiate VASP transactions. Customer Care generally needs to handle such requests and they need an easy way to verify the claims of the customers.

Accounting only for the money at the granularity of any access to short code is insufficient. A way to check the transactions per short code per user is needed.

Under ID-SIS-CSM aggregation, the aggregated VASP logs are likely to show only NameID, but the Customer Care center can be trusted by the operator and thus can map from the NameIDs back to the MSISDN.
6. Using ID-SIS-CSM with MM7 XML Schema

To address a message to multiple recipients, see Section 4.2, the identity addressing tokens MUST be placed in the `<mm7:Extension>` container in the `<To>`, `<Cc>`, or `<Bcc>` container of an MM7 message as if the AddressGroup schema element contained a choice with

```
<xs:element name="Extension" type="mm7:anyDataType"/>
```
7. Examples

The following examples illustrate some ID-SIS-CSM protocol exchanges and the ID-WSF SOAP binding around them. These examples are not normative. In fact, they even make use of the ability to use other versions of MM7 than that specified in [MM7].

7.1. MO Round Trip

Assuming the following plain MM7 message, carried on https transport, on MO2 interface,

```
POST /send.x HTTP/1.0
HOST: 192.168.70.72
SOAPACTION: ""
X-FH-EXTERNAL-MESSAGE-ID: Q0FL6sProLUAEV3AAACQAAAAAMAAAAA
X-FH-CONNECTION-ID: 3184
X-FH-ROUTING-FROM: +44679501170/TYPE=PLMN
CACHE-CONTROL: no-cache
USER-AGENT: demo/1.5
CONNECTION: keep-alive
ACCEPT: text/html, image/gif, image/jpeg, */*; q=.2, */*; q=.2
PRAGMA: no-cache
CONTENT-LENGTH: 1844
CONTENT-TYPE: multipart/related;
boundary="fh-mms-multipart-boundary-11059-1128352777535";
type="text/xml";
start="<cid-550@192.168.115.10>"

--fh-mms-multipart-boundary-11059-1128352777535
Content-Type: text/xml; charset="utf-8"
Content-ID: <cid-550@192.168.115.10>

<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope
xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/"
xmllns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.3gpp.org/ftp/Specs/archive/23_series/23.140/schema/REL-5-MM7-1-0"

<soap-env:Header>
<TransactionID
xmlns="http://www.3gpp.org/ftp/Specs/archive/23_series/23.140/schema/REL-5-MM7-1-0"
xmllns="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.3gpp.org/ftp/Specs/archive/23_series/23.140/schema/REL-5-MM7-1-0.xsd">
<fh-transaction-id-11058-1128352777534

</TransactionID>
</soap-env:Header>
</soap-env:Body>

<DeliverReq
xmlns="http://www.3gpp.org/ftp/Specs/archive/23_series/23.140/schema/REL-5-MM7-1-0"
xmllns="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.3gpp.org/ftp/Specs/archive/23_series/23.140/schema/REL-5-MM7-1-0.xsd">
<MM7Version>5.3.0</MM7Version>
<LinkedID>0001CE41150A4AC</LinkedID>
<Sender>
<Number>44679501170</Number>
</Sender>
<Recipients>
<To>
<ShortCode>55555</ShortCode>
</To>
</Recipients>
<TimeStamp>2005-10-03T15:19:37-00:00</TimeStamp>
<Priority>Normal</Priority>
<Content
allowAdaptations="true"
```
the MO-Relay could send following MO3 message to the IdP.

```
POST /ecplogin HTTP/1.0
SOAPACTION: http://www.oasis-open.org/committees/security
X-MSISDN: 44679501170
CONTENT-TYPE: text/xml

<soap:Envelope
  xmlns:lib="urn:liberty:iff:2003-08"
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header>
    <paos:Request
      xmlns:paos="urn:liberty:paos:2003-08"
      messageID="1"
      responseConsumerURL="https://g-wsc.liberty-iop.org:8643/MM7-CS"
      service="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
      soap:Actor="http://schemas.xmlsoap.org/soap/actor/next"
      soap:mustUnderstand="1"/>
    <ecp:Request
      xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
      IsPassive="0"
      ProviderName="g-wsc"
      soap:Actor="http://schemas.xmlsoap.org/soap/actor/next"
      soap:mustUnderstand="1">
      <sa:Issuer
        xmlns:sa="urn:oasis:names:tc:SAML:2.0:assertion"
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
        https://g-wsc.liberty-iop.org:8643/sp.xml
      </sa:Issuer>
    </ecp:Request>
  </soap:Header>
  <soap:Body>
    <sp:AuthnRequest
      xmlns:sp="urn:oasis:names:tc:SAML:2.0:protocol"
      AssertionConsumerServiceURL="https://g-ecp.liberty-iop.org:8083/SP-P"
      ForceAuthn="false"
      ID="RYjvfbq_BGdjZ1gzD63W"
      IsPassive="false"
      IssueInstant="2005-10-03T16:58:28Z"
      ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS"
      ProviderName="g-wsc"
      Version="2.0">
      <sa:Issuer
        xmlns:sa="urn:oasis:names:tc:SAML:2.0:assertion"
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
        https://g-wsc.liberty-iop.org:8643/sp.xml
      </sa:Issuer>
    </sp:AuthnRequest>
  </soap:Body>
</soap:Envelope>
```
This <AuthnRequest> is synthesized on behalf of the SP whose provider ID is https://g-wsc.liberty-iop.org:8643/sp.xml. Note that the request is performed by the MO-Relay on behalf of another provider (the Content Provider or VASP) and therefore the request is not signed.
The next step in the mobile-originated sequence is that the MO-Relay sends an unsolicited PAOS response (MO5), along with the original MM7 message, to the ID-VASP. The Response is appended after the regular MM7 message (DeliverReq).

The MO5 message might be like:

```
POST /MM7-CS HTTP/1.0
AUTHORIZATION: Basic c3ltbGFiczpzeW1sYWJz
SOAP_ACTION: 
CONTENT-TYPE: multipart/related;
type=text/xml; start="</cmvt256/mm7-submit>";
boundary=1128358710_2078917053
--1128358710_2078917053
```

ID-WSF1.1 DS ResourceOffering with appropriate credentials would go in here

```
<soap:Envelope
 xmlns:lib="urn:liberty:iff:2003-08"
 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
 <soap:Header>
  <mm7:TransactionID
   xmlns:mm7="http://www.3gpp.org/ftp/Specs/archive/23_series/23.140/schema/REL-5-MM7-1-2"
   soap:actor="http://schemas.xmlsoap.org/soap/actor/next"
   soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding"
   soap:mustUnderstand="1">TIDszxsyhQptODEPnpGtCEG</mm7:TransactionID>
 </soap:Header>
 <soap:Body id="bdy">
  <mm7:DeliverReq
   xmlns:mm7="http://www.3gpp.org/ftp/Specs/archive/23_series/23.140/schema/REL-5-MM7-1-2">
   <mm7:MM7Version>5.3.0</mm7:MM7Version>
   <mm7:LinkedID>0001CE41150A4AC</mm7:LinkedID>
   <mm7:Recipients>
    <mm7:To>
     <mm7:ShortCode>55555</mm7:ShortCode>
    </mm7:To>
   </mm7:Recipients>
   <mm7:TimeStamp>2005-10-03T15:19:37-00:00</mm7:TimeStamp>
   <mm7:Priority>Normal</mm7:Priority>
   <mm7:Content
    allowAdaptations="true"
    href="0001CE41150A4AD@demo.com"
    type="MMS"/>
  </mm7:DeliverReq>
 </soap:Body>
</soap:Envelope>
<sp:Response
 xmlns:sp="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="R43axB2w-lIc4g-nSoqZp"
 InResponseTo="RYijvfbg_BGdjZ1gxD63W"
 IssueInstant="2005-10-03T16:58:30Z"
 Version="2.0">
 <sa:Issuer
  xmlns:sa="urn:oasis:names:tc:SAML:2.0:assertion"
  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
   https://g-ds.liberty-iop.org:8681/idp.xml
 </sa:Issuer>
 <sp:Status
  Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</sp:Status>
<sa:Assertion
 xmlns:sa="urn:oasis:names:tc:SAML:2.0:assertion"
 ID="ARFA7ZbsmMf1MY_Cw6S5"
 IssueInstant="2005-10-03T16:58:30Z"
 Version="2.0">
 <sa:Issuer
  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
   https://g-ds.liberty-iop.org:8681/idp.xml
 </sa:Issuer>
 <ds:Signature
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:ds:CanonicalizationMethod
   Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
  xmlns:ds:SignatureMethod
   Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
  xmlns:ds:Reference URI="#ARFA7ZbsmMf1MY_Cw6S5"
  xmlns:ds:Transforms
   xmlns:ds:Transform
    Algorithm="http://www.w3.org/2001/01/xml-exc-c14n#"/>
As may be seen, this message contained a discovery bootstrap with appropriate credentials. This allows the ID-V ASP to contact other ID Web Services as needed to satisfy the request of the Principal. Eventually, the ID-V ASP responds with MO6 which could look like this:

```
HTTP/1.0 200 Ok
CONTENTS: 817
```

As may be seen, this message contained a discovery bootstrap with appropriate credentials. This allows the ID-V ASP to contact other ID Web Services as needed to satisfy the request of the Principal. Eventually, the ID-V ASP responds with MO6 which could look like this:
This message is pretty much a standard MM7 message without any Liberty-specific content. The MO-Relay will then pass this message as the response to MO2. The MMSC will match the response to MO2 using the TransactionID MM7 header.

7.2. MT Round Trip

An ID-SIS-CSM WSC that wishes to send a message to the principal would first use discovery service to discover the end point and credentials for contacting the MT-Relay. Armed with these, it could send an MT3 message like:

POST /MM7-PSBEARER HTTP/1.0
AUTHORIZATION: Basic c3ltbGFiczpzeW1sYWJz
SOAP_ACTION: 
CONTENT-TYPE: multipart/related; type=text/xml;
start="</cmvt256/mm7-submit>";
boundary=1128358715_143302914
--1128358715_143302914
CONTENT-ID: </cmvt256/mm7-submit
CONTENT-TYPE: text/xml; charset="utf-8"

<soap:Envelope
xmlns:lib="urn:liberty:iff:2003-08"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
><soap:Header>
<Correlation S:mustUnderstand="1"
id="uuid:an0CrHcakhhtKqMSozX2"
actor="http://schemas.../next"
messageID="uuid:efefefef-aaaa-ffff-cccc-efffbbbbb"
timestamp="2112-03-15T11:12:12Z"/>
<Provider providerID="https://g-wsc.liberty-iop.org:8643/SP-P"
affiliationID="affiliation.example.com"
S:mustUnderstand="1"
id="A9kendan...542"
actor="http://schemas.../next"/>
<wsse:Security

Liberty Alliance Project

24
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
  <sa:Assertion xmlns:sa="urn:oasis:names:tc:SAML:2.0:assertion">
    <sa:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
      https://g-ds.liberty-iop.org:8681/idp.xml
    </sa:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="#CREDI-6f21BJANxsx8hzWW8D">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>nJXIYiH8Rl6x+aOSK37QdHmzyhQ=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>An+EiTVBQEWKZF5akC...EnEIew=</ds:SignatureValue>
    </ds:Signature>
    <sa:Subject>
      <sa:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">
        PaQUIF0-dqnwIfN9yE92T
      </sa:NameID>
      <sa:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
    </sa:Subject>
    <sa:Conditions NotBefore="2005-10-03T16:53:32Z"
      NotOnOrAfter="2005-10-03T17:08:32Z">
      <sa:AudienceRestriction>
      </sa:AudienceRestriction>
    </sa:Conditions>
    <sa:AuthnStatement AuthnInstant="2005-10-03T16:58:32Z">
      <sa:AuthnContext>
      </sa:AuthnContext>
    </sa:AuthnStatement>
  </sa:Assertion>
</wsse:Security>

<mm7:TransactionID xmlns:mm7="http://www.3gpp.org/ftp/Specs/archive/23_series/23.140/schema/REL-5-MM7-1-2">
  <mm7:SubmitReq soap:actor="http://schemas.xmlsoap.org/soap/actor/next" soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding" soap:mustUnderstand="1">
    TIDUIVaYo8-B0w1GghIi8In
  </mm7:SubmitReq>
</mm7:TransactionID>

<soap:Header>
  <soap:Body id="bdy">
    <mm7:TransactionID xmlns:mm7="http://www.3gpp.org/ftp/Specs/archive/23_series/23.140/schema/REL-5-MM7-1-2">
      <mm7:SubmitReq soap:actor="http://schemas.xmlsoap.org/soap/actor/next" soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding" soap:mustUnderstand="1">TIDUIVaYo8-B0w1GghIi8In</mm7:SubmitReq>
    </mm7:TransactionID>
  </soap:Body>
</soap:Header>
<mm7:Password>symlabs</mm7:Password>

<mm7:SenderAddress>
    <mm7:ShortCode>55555</mm7:ShortCode>
</mm7:SenderAddress>

<mm7:SenderIdentification>
    <mm7:Subject>ID-CSM-DEMO</mm7:Subject>
</mm7:SenderIdentification>

<mm7:To>
    <mm7:Extension>
                http://mt-gw.com/4mOB82k15csaUxs
            </ds:ResourceID>
            <csm:CredentialRef>CREDI-6f21BJANxsx8hzWW8D</csm:CredentialRef>
        </csm:IdentityAddressingToken>
    </mm7:Extension>
</mm7:To>

<mm7:Content href="HREF49vH9ByyRzVzgIPg7EEs"/>

</mm7:SubmitReq>

</soap:Body>
</soap:Envelope>

To load games click http://192.168.160.57/symlabs/games.jad

The SOAP headers and the To: field in the message body contain all the necessary material for determining to whom the message is destined. Note that the <IdentityAddressingToken> in the To: body field points to the assertion in the WS-Security SOAP header.

The MT-Relay will figure out the MSISDN according to this information, perhaps using some other ID Web Service call that is not shown here and is out of scope. Calling these services is facilitated by the fact that the MT3 request contains the discovery bootstrap. Once the MSISDN is known, the MT-Relay will send the MM7 portion of the message to the MMSC (MT4).

POST /mm7extadapter HTTP/1.0
AUTHORIZATION: Basic c3ltbGFiczpzeW1sYWJz
SOAP_ACTION:
CONTENT-TYPE: multipart/related; type=text/xml; start="</cmvt256/mm7-submit">; boundary=1128358716_2078917053

To load games click http://192.168.160.57/symlabs/games.jad

<soap:Envelope
    xmlns:lib="urn:liberty:iff:2003-08"
7.3. MT to Multiple Recipients

This example illustrates sending a message to multiple recipients by listing their `<IdentityAddressingToken>` elements in the `<To>` field in the body of the SOAP message, whilst one or more SAML assertions could be included in the WS-Security header for access control purposes. The `<CredentialsRef>` element links a specific ResourceId with the assertion corresponding to such user.
POST /MM7-PSBEARER HTTP/1.0
Authorization: Basic c3ltbGFiczpzeW1sYWJz
SOAP_ACTION:
CONTENT-TYPE: multipart/related; type=text/xml;
boundary=--1128358715_143302914
--1128358715_143302914
CONTENT-ID: </cmvt256/mm7-submit>
CONTENT-TYPE: text/xml; charset="utf-8"

<soap:Envelope
xmlns:lib="urn:liberty:iff:2003-08"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
><soap:Header>
<wsa:MessageID
xmlns:wsa="http://www.w3.org/2005/03/addressing"
id="#MID">uuid:an0CrHcakhhtKqMSozX2</wsa:MessageID>
</soap:Header>
<Correlation S:mustUnderstand="1"
id="uuid:an0CrHcakhhtKqMSozX2"
actor="http://schemas.../next" messageID="uuid:efefefef-aaaa-ffff-cccc-eeeeffffb bbb"
timestamp="2112-03-15T11:12:12Z"/>
<Provider providerID="https://g-wsc.libr erty-iop.org:8643/SP-P"
affiliationID="affiliation.example.com"
S:mustUnderstand="1"
id="A9kendan...542"
actor="http://schemas.../next"/>
<wse:Security
xmlns:wse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
ty-secext-1.0.xsd">
<sa:Assertion
xmlns:sa="urn:oasis:names:tc:SAML:2.0:assertion"
ID="CREDI-6f21BJAXsx8hzW8D"
IssueInstant="2005-10-03T16:58:32Z"
Version="2.0"/>
<sa:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference URI="#CREDI-6f21BJAXsx8hzW8D"/>
<ds:Transforms>
<ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>nJXIYiH8R16k+aOSK37QdHmzyhQ</ds:DigestValue>
</ds:Reference>
<ds:SignedInfo/>
<ds:SignatureValue>Ann+E1TVBQEWK...EnEIew</ds:SignatureValue>
</ds:Signature>
<sa:Subject>
<sa:NameID
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
NameQualifier="https://mt-relay.liberty-iop.org:8681/wsp.xml">
UVWXYZ</sa:NameID>
<sa:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
</sa:Subject>
<sa:Conditions>
  NotBefore="2005-10-03T16:53:32Z"
  NotOnOrAfter="2005-10-03T17:08:32Z">
  <sa:AudienceRestriction>
  </sa:AudienceRestriction>
</sa:Conditions>
<sa:AuthnStatement AuthnInstant="2005-10-03T16:58:32Z">
  <sa:AuthnContext>
    <sa:AuthnContextClassRef>
      urn:oasis:names:tc:SAML:2.0:ac:classes:Password
    </sa:AuthnContextClassRef>
  </sa:AuthnContext>
</sa:AuthnStatement>
</sa:Assertion>
<sa:Assertion xmlns:sa="urn:oasis:names:tc:SAML:2.0:assertion"
ID="CREDI-1234156154574djask"
IssueInstant="2005-10-03T16:58:32Z"
Version="2.0">
  <sa:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
    https://g-ds.liberty-iop.org:8681/idp.xml
  </sa:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <ds:Reference URI="#CREDI-1234156154574djask"/>
      <ds:Transforms>
        <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>nJXIYiH8Rl6x+aOSK37QdHmzyhQ=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>An+EiTV...BcOEnEIEW=</ds:SignatureValue>
</ds:Signature>
<sa:Subject>
  <sa:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
NameQualifier="https://mt-relay.liberty-iop.org:8681/wsp.xml">
    PaQU1f0-dqwn0F9yE92T
  </sa:NameID>
  <sa:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
</sa:Subject>
<sa:Conditions>
  NotBefore="2005-10-03T16:53:32Z"
  NotOnOrAfter="2005-10-03T17:08:32Z">
  <sa:AudienceRestriction>
  </sa:AudienceRestriction>
</sa:Conditions>
<sa:AuthnStatement AuthnInstant="2005-10-03T16:58:32Z">
  <sa:AuthnContext>
    <sa:AuthnContextClassRef>
      urn:oasis:names:tc:SAML:2.0:ac:classes:Password
    </sa:AuthnContextClassRef>
  </sa:AuthnContext>
</sa:AuthnStatement>
<sa:AuthnStatement>
</sa:Assertion>
</wsse:Security>

<mm7:TransactionID xmlns:mm7="http://www.3gpp.org/ftp/Specs/archive/23_series/23.140/schema/REL-5-MM7-1-2" soap:actor="http://schemas.xmlsoap.org/soap/actor/next" soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding" soap:mustUnderstand="1">TIDV5aYo8-B0w1GphIi8In</mm7:TransactionID>

</soap:Header>
<soap:Body id="bdy">

<mm7:SubmitReq xmlns:mm7="http://www.3gpp.org/ftp/Specs/archive/23_series/23.140/schema/REL-5-MM7-1-2">

<mm7:MM7Version>5.3.0</mm7:MM7Version>
<mm7:SenderIdentification>

<mm7:VASPID>symlabs</mm7:VASPID>
<mm7:Password>symlabs</mm7:Password>
<mm7:SenderAddress>

<mm7:ShortCode>55555</mm7:ShortCode>
</mm7:SenderAddress>
</mm7:SenderIdentification>

<mm7:To>

<mm7:Extension>


http://mt-gw.com/4mOB82k15csaUxs</ds:IdentityAddressingToken>
</mm7:Extension>

</mm7:To>

<mm7:Subject>ID-CSM-DEMO</mm7:Subject>

<mm7:Content href="HREF49vH9ByyRzVzgIPg7EEs"/>
</mm7:SubmitReq>

</soap:Body>

</soap:Envelope>

--1128358715_143302914
CONTENT-ID: HREF49vH9ByyRzVzgIPg7EEs
CONTENT-TYPE: multipart/mixed; boundary=1128358715_2078917053

--1128358715_2078917053
CONTENT-TRANSFER-ENCODING: base64
CONTENT-TYPE: image/gif
R0lGODlhGQA1AIQAAP/3SUqvJpE8OFBBuIgDvUMAADs=

--1128358715_2078917053
CONTENT-TYPE: text/plain; charset=UTF-8
To load games click
http://192.168.160.57/symlabs/games.jad

--1128358715_2078917053--
--1128358715_143302914--
8. Annex: Legacy Messaging Features

This informational annex contains further guidance about how to combine an optional extension of the MM7 protocol with the Liberty identity wrapper, providing such optional extension a unified messaging mechanism which complements the standard MM7 protocol.

8.1. Representation of Content

1. The ID-SIS-CSM messages SHOULD represent the contents of the message as a MIME multipart. The MM7 <Content> element SHOULD contain a reference to the Content-ID of the corresponding MIME multipart.

2. The MM7 <Content> element SHOULD have type XML attribute that indicates the type of multimedia content present. Possible values are:

   - MULTIMEDIA_HIGH: MMS content
   - MULTIMEDIA_LOW: EMS or NSM content
   - TEXT: SMS content

Additional values may be defined in future specifications. Experimental and non-official values MUST start by "X-", e.g., X-MY-FORMAT.

An example of an MM7 <Content> element is:

```xml
<mm7:Content href="HREF49vH9ByyRzVzgIPg7EEs" type="MULTIMEDIA_HIGH"/>
```

See the full examples for illustrations of the MIME multipart structure.

8.2. SMS Support

Additional [SMS] messaging parameters can be passed as attribute-value Pairs using the <MessageExtraData> element.

- **Mode**: Message processing mode. Either transparent or notTransparent.
- **SMSText**: Alternate representation of SMS message content.
- **DataCodingScheme**: How message content is encoded. If in conflict with SMSMessageClass, the latter shall prevail.
- **SMSMessageClass**: Indication of call of the message, affecting presentation and retention of the message. See [SMS] for further details.
- **UserDataHeader**: Allows indication of SMS message headers.
- **UserData**: Message content in binary.
- **ProtocolIdentifier**: Allows the protocol to be identified for SMS messages.
- **SIMSubstitution**: Boolean (true or false) that indicates whether a message on SIM card should be substituted by the present message. By default, the message in slot 0 is substituted. Other slots can be indicated using ProtocolIdentifier.
8.3. Indication of Sending Preferences for MT

If the ID-SIS-CSM WSC wishes to indicate sending preferences, it should include `<PreferredChannels>` element. It contains a list of technologies in order of preference. Possible technologies are:

- SMS
- MMS
- WAPPUSH

These only indicate preference. The message should be sent using the first technology that is compatible with the type of the content. If none of the preferred technologies are compatible, the behavior is implementation-dependent. The implementation may send it anyway using a technology that is compatible, but not listed, or it may reformat the message to match one of the preferred technologies, or it may report an error.

Example

```xml
<mm7:PreferredChannels>
  <mm7:DeliverUsing>MMS</mm7:DeliverUsing>
  <mm7:DeliverUsing>SMS</mm7:DeliverUsing>
</mm7:PreferredChannels>
```

8.4. Support for WAP Push

For improved WAP Push support, the ID-SIS-CSM WSC may include in the `<MessageExtraData>` element the following information as attribute-value pairs.

- **WAPushType** Indicates the type of WAP Push message, such as `ServiceIndication` or `ServiceLoading`. See [WAPUSH] for further information.
- **WAPushURL** Indicates message URL.
- **WAPushText** WAP Push message to be shown to user for ServiceIndication messages.
- **WAPushID** Message ID for WAP Push.
- **WAPushAction** The action that the terminal should take upon receiving a WAP Push message. For ServiceIndication messages, this can be:
  - `signal-none`
• signal-low
• signal-medium
• signal-high

For ServiceLoading messages, this can be:

• execute-low
• execute-high
• cache

8.5. MMStatus Indications Regarding State of the Message

The following additional values for \(<\text{MMStatus}\>\), when used as \(\text{mmDeliveryStatusType}\), are defined:

Processing Message has been received, but may not have been sent to the terminal yet.
Canceled Message has been canceled.
Replaced Message has been replaced.
Delivered Message has been delivered to the user.

Implementations and deployments MAY define additional \(<\text{MMStatus}\>\) values, provided that such values start by an "X-" prefix. No future official status value will start by this prefix.

8.6. Querying State of MT messages

Once a message has been sent by VASP, it can query the state of the messages using the \(<\text{QueryStatusReq}\>\) method.

The message contains the following elements.

TransactionID A SOAP header that provides unique identification of the operation.
MessageType Carried in SOAP body, indicates the type of the operation.
MM7Version MM7 version indicator.
VASPID Identification of the VASP.
VASID Identification of the VAS.
MessageID Identifier of the message whose status is being queried.

The status query is replied with the response element \(<\text{QueryStatusRsp}\>\). The following sub-elements are of interest.

TransactionID A SOAP header that provides unique identification of the operation.
MessageType Carried in SOAP body, indicates the type of the operation.
MM7Version MM7 version indicator.
StatusCode Indication of the success of the operation.
StatusText A human-readable description of the error code.
Details
Optional free-format data to capture implementation-specific details.

8.7. Additional Schema to Support Legacy Messaging

To use SMS messages, see Section 8.2, or WAP Push, see Section 8.4. The `<csm:MessageExtraData>` MUST be placed in an `<mm7:Extension>` container in the MM7 message as if the `genericRSReqType`, `genericVASPRequestType`, and `genericResponseType` schemata contained

```
<xs:element name="Extension" type="mm7:anyDataType"
  minOccurs="0" maxOccurs="unbounded"/>
```

as the last member of the sequence.

The `<csm:MessageExtraData>` container is described by the following schema.

```
<xs:complexType name="messageExtraDataType">
  <xs:sequence maxOccurs="unbounded">
    <xs:element name="element" type="csm:elementType"/>
  </xs:sequence>
</xs:complexType>
```

```
<xs:complexType name="elementType">
  <xs:sequence>
    <xs:element name="key" type="xs:string">
      <xs:element name="value" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
```

Liberty Alliance Project
References

Normative


[MM7] "TS 23.140: Multimedia Messaging Service (MMS); Functional Description; Stage 2 (Release 6)," 3GPP v6.a.0 (2005-06), (June, 2005). http://www.3gpp.org/ftp/Specs/archive/23_series/23.140/23140-6a0.zip


http://www.w3.org/TR/xmlschema-1/

[SMS] "TS 03.40: Technical Realization of the Short Message Service (SMS)," 3GPP v7.5.0, (December, 2002).
http://www.3gpp.org/ftp/Specs/archive/03_series/03.40/0340-750.zip

[SOAPattach] "SOAP Messages with Attachments," Barton, John, Thatte, Satish, Nielsen, Henrik Frystyk, eds.


"Web Services Security: SOAP Messages with Attachments (SwA) Profile 1.1," OASIS Standard, 01 February, 2006,

[XML] Bray, Tim, Paoli, Jean, Sperberg-McQueen, C. M., Maler, Eve, Yergeau, Francois, eds. (04 February 2004).
"Extensible Markup Language (XML) 1.0 (Third Edition)," Recommendation, World Wide Web Consortium
http://www.w3.org/TR/2004/REC-xml-20040204

Informative
