igovt logon service

Context Mapping Service (iCMS) Messaging Specification

Release 9.6

Subject	Context Mapping Service Messaging Specification for the igovt logon service
Client	The Department of Internal Affairs
Author	Datacom Systems (Wellington) Limited
Date	05 Dec 2012
Version	1.0
Status	Pending update to RealMe
Classification	In Confidence

Table of Contents

1. Introduction

1.1 Overview

This document specifies the Context Mapping Service interface exposed by the igovt logon service to integrating Service Providers.

1.2 Document Purpose

This document has been created to describe the interface that exists between the Context Mapping Service and a Service Provider's application ('the SP').
This document serves two key purposes:

1. It describes the messaging interfaces sufficiently for third party software developers to design and build SA-based interfaces to the Context Mapping Service;

2. It describes the messaging interfaces sufficiently for the solution vendor to develop the interfaces.

This document will be used to describe a web service interface built up from message elements from WS-Trust 1.4, and the use of this interface in a sequence of message exchanges.

1.3 Document References

The following SAML references are used throughout this document:

Reference	Name	Description
saml-core-2.0-os	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) v2.0	The core SAML 2.0 specification from OASIS. Usage constrained by [nzsams].

These documents can be found at http://docs.oasis-open.org/security/saml/v2.0/

The following igovt logon service references are used throughout this document:

Reference	Name	Description
ils-saml20-1.7.2	igovt logon service SAML v2.0 Messaging Specification Release 8 1.6.5.	Describes the SAML 2.0 Web SSO solution implemented for the igovt logon service.
icms-int-guide	Context Mapping Service Integration Guide	A guide for SP integrating to the Context Mapping Service using WS-Trust 1.4. Contains the specific technical steps and requirements for an integrator to follow.
ils-int-guide	SAML2 igovt logon service Integration Guide v1.5	A guide for SP integrating to the igovt logon service using SAML v2.0. Contains the specific technical steps and requirements for an integrator to follow.

The following WS-* references are used throughout this document:

Reference	Name	Description
ws-trust-1.3	WS-Trust 1.3	WS-* specification from OASIS defining messaging elements for security token exchange.
ws-trust-1.4	WS-Trust 1.4	WS-* specification from OASIS defining extra messaging elements for security token exchange.
ws-addressing-1.0	WS-Addressing 1.0	WS-* specification from OASIS defining messaging elements for the SOAP header that define senders, recipients, and actions.

The following third party references are used throughout this document:

Reference	Name	Description
nzsams	New Zealand Security Assertion Messaging Standard. (June 2008 version 1.0 - ISBN 978-0-478-30344-5)	Prescribes messaging standards for communicating a range of security assertions (authentication, identity attributes and authorisation) in New Zealand government online services.
xml-schema-datatypes	XML Schema Part 2: Datatypes. (http://www.w3.org/TR/xmlschema-2/.)	XML Schema datatypes

Reference	Name	Description
nzsit-402	NZ ICT Security Manual NZSIT 402:2007	NZ ICT Security Manual Authored by Government Communications Security Bureau
RFC2119	Key words for use in RFCs to Indicate Requirement Levels (http://www.ietf.org/rfc/rfc2119.txt)	Defines the meanings of the key words SHOULD, MUST etc. that appear in capital letters through this document.

Where these documents are referenced they will be surrounded by [ ] to contain the reference name. e.g. [saml-core-2.0-os].

1.4 Definitions

The following abbreviations will be used for the terms in the above documents listed in section 1.3.

Acronym or term	Description
Base64	**Base64:** A data encoding scheme whereby binary-encoded data is converted to printable ASCII characters. The only characters used are the upper- and lower-case Roman alphabet characters (A–Z, a–z), the numerals (0–9), and the "+" and "/" symbols, with the "=" symbol as a special suffix code.
DIA	**The Department of Internal Affairs:** responsible for running the igovt logon service.
FLT	**Federated Logon Tag** A synonym for the SAML NameID (previously referred to as MCSN). Used in a SAML assertion identity the authenticated user in a federated environment.
igovt logon service	**igovt logon service:** This is the term used to refer to the system (software, infrastructure and help desk) commissioned by the State Services Commission in the Shared Logon Initial Implementation Project. This system has also been referred to as the Common Logon Service, Common Logon Site, the Shared Logon Initial Implementation Solution and the Government Logon Service.
HTTP	**HyperText Transfer Protocol:** A protocol for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.
HTTPS	**HTTP over SSL:** A protocol which uses of Netscape's Secure Socket Layer (SSL) as a sub-layer under its regular HTTP application layering.
Logon	A igovt logon service credential. Used interchangeably with 'credential'.
Logon Attributes Token	A token issued as an attribute of the SAML token issued by the igovt logon service, and provides assurance of a user's identity and recent activity to the Context Mapping Service.
MCSN	**Modified Credential Serial Number** A previously used term for the SAML NameID (or FLT).
Mutual SSL	Mutual SSL refers to two parties authenticating each other suitably using digital signatures. The client authenticates themselves to a server and that server authenticates itself to the client in such a way that both parties are assured of the others' identity by digital signatures. Mutual SSL provides the same things as SSL, with the addition of authentication and non-repudiation of the client and server using digital signatures. Mutual SSL is also known as Client TLS or Client SSL.
NTP	**Network Time Protocol:** A protocol to exchange and synchronize time on computer networks.

Acronym or term	Description
Opaque Token	A token issued but the Context Mapping Service that can be used to pass a user identity from a source Service Provider to a target Service Provider without exposing the FLT for either Service Provider to the other Service Provider, and without establishing anything that could be used as a shared identifier.
Privacy Domain	A privacy domain is a SAML v2.0 NameID generation space. SP's that reside in the same privacy domain will be returned the same SAML v2.0 NameID in the Assertion of the user's logon in the SAML response.
Redeem Token	A token issued by the Context Mapping Service that asserts a user's identity in form that a target service provider can read.
SAML	**Security Assertion Markup Language:** SAML is an OASIS standard that defines a framework for exchanging security assertions (described in XML) between online partners.
SOAP	**Simple Object Access Protocol:** A lightweight protocol that defines how information may be exchanged in a distributed and decentralized environment using XML.
SP	**Service Provider.** A role donned by a system entity where the system entity provides services to principals or other system entities.
SSL	**Secure Socket Layer:** A protocol for transmitting sensitive information across the Internet in a secure way. The later TLS standard may also be used instead of SSL.
TLS	**Transport Layer Security.** TLS and its predecessor, (SSL), are cryptographic protocols that provide secure communications on the Internet. There are slight differences between SSL and TLS, but the protocol remains substantially the same. TLS is based on SSL 3.0.
XML	**Extensible Markup Language:** A markup language for Internet documents which allows designers to create their own tags (hence extensible).
UTC	**Coordinated Universal Time:** An international, highly accurate and stable uniform atomic time system.
User Agent	Software that end users operate to access the services. Typically this is a web browser.

1.5 XML Name Spaces

The following name spaces and name space prefixes are used in sample messages.

Prefix	Name Space
wst	http://docs.oasis-open.org/ws-sx/ws-trust/200512
wst14	http://docs.oasis-open.org/ws-sx/ws-trust/200802
wsp	http://schemas.xmlsoap.org/ws/2004/09/policy
wsa	http://www.w3.org/2005/08/addressing
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
saml2	urn:oasis:names:tc:SAML:2.0:assertion
env	http://www.w3.org/2003/05/soap-envelope
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
wsse11	http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd
wsa	http://www.w3.org/2005/08/addressing
iCMS	urn:nzl:govt:ict:stds:authn:deployment:igovt:gls:iCMS:1_0

1.6 Assumptions

This document assumes the reader has:

- a working knowledge of the documents listed in section 1.3 and
- an appreciation of the terms and abbreviations used in the documents listed and in section 1.4.

1.7 Notation

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 IETF RFC 2119 [RFC2119].

1.8 Specification Compliance

For an implementation or deployment to call itself compliant with this specification it MUST satisfy all aspects of this document marked as MUST as well as all conformance and specification requirements of the following specifications that are relevant to the functionality covered in this document:

- WS-Trust 1.4
- WS-Security 1.2
- SOAP 1.2
- WS-Addressing 1.0

2. Messaging Overview

The Context Mapping Service exposes a WS-Trust 1.4 interface for Service Providers to obtain security tokens that identify users during message exchanges with other Service Providers integrated with the igovt logon service.

The purpose of the igovt logon service is to authenticate users to Service Providers without Service Providers sharing any common identifiers for the users. This prevents Service Providers from being able to easily correlate data about the user. It also prevents Service Providers from implementing web services for each other that can be composed into beneficial applications for users

The Context Mapping Service provides a mechanism that permits a Source Service Provider to transmit a user identity to a Target Service provider with the restriction that neither Service Provider will have access to the FLT for the other Service Provider. It does this by issuing a token, which only it can read, representing the user. This opaque token is passed from the source Service Provider to the target Service Provider, and then passed back to the Context Mapping Service which then be able to tell the target service provider which user the token represents.

WS-Trust 1.4 is a flexible specification with bindings for issuing and validating tokens. It supports any type of token and provides general purpose protocol elements and bindings that could be used in a variety of scenarios. This messaging specification will limit the use to SAML 2.0 tokens, as issued by the igovt logon service, and describe the use of WS-Trust 1.4 in the implementation of the Context Mapping Service.

The igovt logon service issues SAML 2.0 tokens containing logon attribute tokens as the result of user authentication during an implementation of the Web Browser SSO Profile [saml-profiles-2.0-os].

The Context Mapping Service issues two types of security tokens, both which will be SAML 2.0 assertions:

- Opaque Token – The service provider will invoke the Opaque Token operation of the Context Mapping Service to obtain a token for other service providers. The Context Mapping Service will issue an opaque token that can only be processed by the Context Mapping Service's Redeem Token operation.
- Redeem Token – The target service provider will invoke the Redeem Token operation of the Context Mapping Service to redeem the received opaque token from the requesting service provider. The Context Mapping Service will issue a token that is compatible with those issued by the igovt logon service, including being passed to the Opaque Token operation to obtain tokens that can be passed to other service providers.

2.1 Scope

2.1.1 In Scope

This specification will describe the token issuance exchange between the source Service Provider and Context Mapping Service, and the token validation exchange between the target Service Provider and the Context Mapping Service. These exchanges correspond to the Issuance (§4) and Validation (§7) bindings in [ws-trust-1.4].

This specification will describe how the messages are secured. It will provide specific messaging and transport bindings with guarantees of security and confidentiality.

2.1.1 Out of Scope

The Renew (§5) and Cancel (§6) bindings from [ws-trust-1.3] are not used in the implementation of the Context Mapping Service and this specification does not refer to them.

Although the purpose of the specification is to describe how a source Service Provider may acquire a token that can be passed to a target Service Provider, how the token is passed is out of scope. There

is no prescription on how the source Service Provider and target service provider interact, including communications, trust relationships, and exchange of system entity identifiers.

This specification does not describe the full details of the opaque token issued by the Context Mapping Service. It will be a SAML 2.0 token to facilitate transport in WS-Security headers, and will keep the user's identity secure, but the source Service Provider and the target Service Provider MUST NOT rely on the internal structure of it.

Attributes and Elements not explicitly mentioned in this specification are not used in the implementation of the Context Mapping Service and therefore do not have defined behaviours.

Messaging Pre-Requisites

There are certain pre-requisites that MUST be completed prior to interfacing with the production Context Mapping Service. These will be defined in full in the Context Mapping Service Integration Guide [iCMS-int-guide] but to assist with integration the following summary is provided:

2.1.2 Integrate with the igovt logon service

Service providers MUST be integrated with the igovt logon service. The Context Mapping Service translates the logon attribute tokens issued by the igovt logon service. Refer to [ils-saml20-1.7.2] and [ils-int-guide] for details.

2.1.3 Mutual SSL Certificates

Mutual SSL will be used to convey the WS-Trust messages. The Service Provider MUST provide the DIA igovt logon service Operations Manager with their client certificate and the igovt logon service SHALL provide each Service Provider with the igovt logon service server certificate for this exchange.

The mutual SSL certificate MUST be distinct from the SAML messaging certificate.

The algorithm used to generate key pairs MUST be RSA[1]. The reference [ils-int-guide] contains further information on the precise types of certificates that are accepted.

2.1.1 WS-Trust Messaging Certificates.

The service providers MUST have Messaging Certificates to sign requests to the Context Mapping Service. The Messaging Certificates MUST be present in the service provider's SAML metadata.

The algorithm used to generate key pairs MUST be RSA[2]. The reference [ils-int-guide] contains further information on the precise types of certificates that are accepted.

2.1.2 Server Synchronisation

The SP's application server's system clock MUST be synchronised with a time source that is in synchronisation with the igovt logon service's time source in order to ensure the limited life time of the sender's message is not exceeded due to system time variations.

To fulfil this requirement synchronisation with a NTP server that is in synchronisation with the igovt logon service's time source is RECOMMENDED. The reference [ils-int-guide] contains further information on synchronisation time sources.

[1] This will conform to [nzsit-402].
[2] This will conform to [nzsit-402].

3. Common Message Bindings

This section gives details of the aspects of transport and messaging that is common to all request and reply messages.

3.1 Transport

The messages MUST use SOAP 1.2 over HTTP 1.1 for transport. The HTTP 1.1 transport layer SHALL be encrypted. Both the Context Mapping Service and Service Provider making the request MUST use X.509 certificates to identify themselves to each other. Transport encryption MUST be implemented with one of the following specifications:

- SSL v3
- TLS 1.0
- TLS 1.1
- TLS 1.2

The X.509 certificates used to secure the transport and provide mutual identification of the participating parties MUST be distinct from the SOAP messaging certificates. The X.509 certificates MUST carry RSA public keys. The Service Provider client certificate MAY be the same certificate used to provide client authentication to the igovt logon service SAML endpoints. The process of certificate exchange is out of scope for this specification.

The SOAPAction HTTP header MUST be provided for all request messages. The value MUST be the same as the value of WS-Addressing Action header for the request.

3.2 Request WS-Addressing

Request messages MUST use WS-Addressing 1.0. WS-Addressing elements are headers, contained, as child elements, in the SOAP header. The following table summarises their use in the Context Mapping Service.

Attribute / Element	WS-Addressing v1.0 Requirement	Context Mapping Service Requirement
To	MAY be provided. See [ws-addressing-1.0]	If provided, the value must either be the endpoint address of the web service or http://www.w3.org/2005/08/addressing/anonymous
From	MAY be provided. See [ws-addressing-1.0]	As per WS-Addressing v1.0 requirement.
ReplyTo	MAY be provided. See [ws-addressing-1.0]	MUST NOT be provided.
FaultTo	MAY be provided. See [ws-addressing-1.0]	MUST NOT be provided.
Action	MUST be provided. See [ws-addressing-1.0]	MUST be provided. The value to be provided is defined the relevant sections of this document for individual messages.
MessageID	MAY be provided. See [ws-addressing-1.0]	MUST be provided.
RelatesTo	MAY be provided. See [ws-addressing-1.0]	As per WS-Addressing v1.0 requirement.

3.3 Response WS Addressing

Response messages MUST use WS-Addressing 1.0. WS-Addressing elements are headers, contained, as child elements, in the SOAP header. The following table summarises their use in the Context Mapping Service.

Attribute / Element	WS-Addressing v1.0 Requirement	Context Mapping Service Requirement
To	MAY be provided. See [ws-addressing-1.0]	If the request message supplied a ReplyTo value other than http://www.w3.org/2005/08/addressing/anonymous then this value MUST be used for the reply message To header.
From	MAY be provided. See [ws-addressing-1.0]	As per WS-Addressing v1.0 requirement.
ReplyTo	MAY be provided. See [ws-addressing-1.0]	MUST NOT be provided.
FaultTo	MAY be provided. See [ws-addressing-1.0]	MUST NOT be provided.
Action	MUST be provided. See [ws-addressing-1.0]	MUST be provided. The value to be provided is defined the relevant sections of this document for individual messages.
MessageID	MAY be provided. See [ws-addressing-1.0]	MUST be provided.
RelatesTo	MAY be provided. See [ws-addressing-1.0]	MUST be provided. The value MUST be same as the value of the MessageID supplied in the request message. The RelationshipType attribute MUST either be omitted or supplied with a value of http://www.w3.org/2005/08/addressing/reply.

3.4 WS-Security

Every input or output message MUST contain a WS-Security 1.1 SOAP header.

The security header MUST contain a Timestamp element, which MUST conform to [wsi-basicsecurityprofile-1.1] §7. In addition, the timestamp MUST have an Expires element. The value of the Expires element MUST NOT be more than 5 minutes after the value of the Created element.

The security header MUST contain a Signature. The signature MUST reference:

- All WS-Addressing headers in the SOAP header.
- The Timestamp element in the WS-Security header.
- The SOAP body.

The signature MAY reference other message parts.

The signature MUST be generated with the private key associated with the senders WS-Trust messaging certificate.

Security Token References to WS-Trust messaging certificates must be SHA1 thumbprint key identifiers.

Service Providers will be identified with SAML 2.0 entity identifiers in SAML 2.0 tokens and WS-Addressing endpoint references, which will be carried in request messages to the Context Mapping Service. The SAML metadata provided to the igovt logon service will associate these entity identifiers with the messaging certificates of the Service Providers, and the Context Mapping Service will enforce this association.

4. The Opaque Token Request

The Opaque Token Request contains a message from a Service Provider requesting a token to allow it to act as a user when using the services of another service provider. This corresponds to step 1 in section 8 of this document.

The messaging is defined as follows.

4.1 Protocol Binding

The value of the WS-Addressing Action header MUST be http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue. The root element contained in the SOAP body MUST be a **RequestSecurityToken** message.

This is described in [ws-trust-1.4] §4.

4.2 Message Elements

Element <RequestSecurityToken>

This message will contain the following elements and attributes:

Attribute / Element	WS-Trust v1.4 Requirement	Context Mapping Service Requirement
Context	MAY be provided.	MAY be provided for messages containing one RequestSecurityToken element.
TokenType	MAY be provided. If not, then it is RECOMMENDED that AppliesTo be used to indicate the target service.	MAY be provided. If it is provided then the value MUST be http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0.
RequestType	MUST be provided and contain the value of 'http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue'.	As per WS-Trust v1.3 requirement.
AppliesTo	MAY be provided.	MUST be provided. The value of the address element MUST be the system entity identifier of the service that the requester intends to present the issued token to.
Claims	MAY be provided.	MUST be provided. The dialect attribute must have a value of 'urn:nzl:govt:ict:stds:authn:deployment:igovt:gls:iCMS:1_0'.
Lifetime	MAY be provided.	As per WS-Trust v1.3 requirement.

Attribute / Element	WS-Trust v1.4 Requirement	Context Mapping Service Requirement
Lifetime/Created	MAY be provided.	MUST be provided. MUST be the instant the request is created. The Context Mapping Service will not support post-dated tokens. Note that the Lifetime element containing the Created element is optional. A creation time may be omitted by not supplying the enclosing Lifetime element.
Lifetime/Expires	MAY be provided.	MUST be provided. Note that the Lifetime element containing the Expires element is optional. An expiration time may be omitted by not supplying the enclosing Lifetime element.
ActAs	MAY be provided as a custom element from an external namespace. See [ws-trust-1.4] §9.3	MUST be provided. Refer to section 4.3 for rules on accepted tokens.

Element <Claims>

This element is REQUIRED.

Attribute / Element	Context Mapping Service Requirement
Consent	MUST be provided. The element content MUST be one of the following identifiers from §8.4 of [saml-core-2.0-os]: • urn:oasis:names:tc:SAML:2.0:consent:current-explicit
TokenSubType	MUST be provided. The element content MUST be one of the following identifiers: • urn:nzl:govt:ict:stds:authn:deployment:igovt:gls:iCMS:1_0::SAMLV2.0: Authenticated • urn:nzl:govt:ict:stds:authn:deployment:igovt:gls:iCMS:1_0:SAMLV2.0: Delayed • urn:nzl:govt:ict:stds:authn:deployment:igovt:gls:iCMS:1_0:SAMLV2.0: Seamless

.

4.3 Accepted Tokens

The content of the ActAs element MUST be a SAML 2.0 token issued by the igovt logon service. The accepted token types are:

- Logon Attributes Token – A SAML token returned as an attribute of the igovt logon service logon token. Refer to [ils-saml20-1.7.2].
- Authenticated Token – A SAML token returned in a Validate Token Response following the issue of an Authenticated opaque token.
- Delayed Token – A SAML token returned in a Validate Token Response following the issue of a Delayed opaque token.

The type of token accepted depends on the value of the TokenSubType claim.

TokenSubType	Accepted Token Types
Authenticated	Logon Attributes Token, Authenticated Token
Delayed	Logon Attributes Token, Delayed Token
Seamless	Logon Attributes Token

4.4 Sample Request

The following is a sample Opaque Token Request message:

```
<env:Envelope>
   <env:Header>
      <wsa:Action>http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue</wsa:Action>
      <wsse:Security>
         <!-- ... -->
      </wsse:Security>
   </env:Header>
   <env:Body>
      <wst:RequestSecurityToken>
         <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</wst:RequestType>
         <wsp:AppliesTo>
            <wsa:EndpointReference>
               <wsa:Address>https://sample-sp-1.govt.nz/realm/samlapp1</wsa:Address>
            </wsa:EndpointReference>
         </wsp:AppliesTo>
         <wst:Claims Dialect="urn:nzl:govt:ict:stds:authn:deployment:igovt:gls:iCMS:1_0">
            <iCMS:Consent>urn:oasis:names:tc:SAML:2.0:consent:current-
explicit</iCMS:Consent>
            <iCMS:
TokenSubType>urn:nzl:govt:ict:stds:authn:deployment:igovt:gls:iCMS:1_0#Authenticated</iCM
S:TokenSubType>
         </wst:Claims>
         <wst:Lifetime>
            <wsu:Created>2010-09-23T22:36:47Z</wsu:Created>
            <wsu:Expires>2010-09-23T22:51:47Z</wsu:Expires>
         </wst:Lifetime>
         <wst14:ActAs>
            <saml2:Assertion IssueInstant="2010-09-23T22:36:47Z"
ID="fcad03b7332bb4143c5d6e602df92e58" Version="2.0">
               <saml2:Issuer>https://www.i.govt.nz/saml2</saml2:Issuer>
               <!-- ... -->
            </saml2:Assertion>
         </wst14:ActAs>
      </wst:RequestSecurityToken>
   </env:Body>
</env:Envelope>
```

5. The Opaque Token Response

The Opaque Token Response contains a message providing a token to the source Service Provider. The token can be passed from the source Service Provider to a target Service Provider, to identify an igovt logon service user, without either Service Provider having access to the other's FLT, and without creating a shared identifier for the user. The returned token will be bound to the target Service Provider so that the Context Mapping Service Validation operation will only accept it if the target Service Provider make the validate request. This corresponds to step 2 in section 8 of this document.

5.1 Protocol Binding

The value of the WS-Addressing Action header MUST be http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal. The root element contained in the SOAP body of a successful response from MUST be a single **RequestSecurityTokenResponseCollection** element. Negotiation or multi-leg authentication is not supported.

5.2 Message Elements

Element <RequestSecurityTokenResponseCollection>

This message will contain the following elements and attributes:

Attribute / Element	WS-Trust v1.4 Requirement	Context Mapping Service Requirement
RequestSecurityTokenResponse	One or more MUST be provided.	As per WS-Trust v1.3 requirement. Note, as per the WS-Trust specification, there is no ordering guarantee on the RequestSecurityTokenResponse elements. Context attributes must be used for correlation.

Element <RequestSecurityTokenResponse>

This message will contain the following elements and attributes:

Attribute / Element	WS-Trust v1.4 Requirement	Context Mapping Service Requirement
Context	MAY be provided, but if the corresponding RequestSecurityToken element provided a value for Context, then it MUST be echoed here.	As per WS-Trust v1.3 requirement.
TokenType	MAY be provided.	MUST be provided. MUST be http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0. Note, while the token is a SAML 2.0 token, it is not intended to be understood by either the source or target Service Provider.

Attribute / Element	WS-Trust v1.4 Requirement	Context Mapping Service Requirement
RequestedSecurityToken	MAY be provided	MUST be provided. The content SHALL be the opaque token that the source Service Provider is to pass to the target Service Provider.
AppliesTo	MAY be provided. SHOULD be provided if the request supplied a value.	MUST be provided. MUST be the same as the value supplied in the request.
RequestedAttachedReference	MAY be provided.	MUST be provided. The Context Mapping Service will enable the source Service Provider to insert SecurityTokenReferences into a message without having to know anything about the structure of the opaque token. However, the opaque token provides no keying material usable by Service Providers, so the SecurityTokenReferences cannot be used in XML Digital Signature or XML Encryption.
RequestedUnattachedReference	MAY be provided.	MUST NOT be provided. The Context Mapping Service does not provide access to tokens outside of the issue request.
RequestedProofToken	MAY be provided.	MUST NOT be provided. The returned token WILL NOT have the source Service Provider as the subject. Establishment of trust relationships between Service Providers is out of scope for this messaging specification.
Entropy	MAY be provided.	MUST NOT be provided. The Context Mapping Service does not support encryption key generation.
Lifetime	MAY be provided.	MUST be provided. MUST have the same values as the returned token.
Lifetime/Created	MAY be provided.	MUST be provided. MUST have the same value as the returned token.
Lifetime/Expires	MAY be provided.	MUST be provided. MUST have the same value as the returned token.

.

5.3 Sample Response

The following is a sample Opaque Token Response message:

```
<env:Envelope>
   <env:Header>
      <wsa:Action>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RSTRC/IssueFinal</wsa:Action>
      <wsse:Security>
         <!-- ... -->
      </wsse:Security>
   </env:Header>
   <env:Body>
```

```
      <wst:RequestSecurityTokenResponseCollection>
         <wst:RequestSecurityTokenResponse>
            <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</wst:TokenType>
            <wst:RequestedSecurityToken>
               <saml2:Assertion IssueInstant="2010-09-23T22:36:47Z"
ID="b7332bb4143c5d6e60fcad032df92e58" Version="2.0">
                  <!-- ... -->
               </saml2:Assertion>
            </wst:RequestedSecurityToken>
            <wsp:AppliesTo>
               <wsa:EndpointReference>
                  <wsa:Address>https://sample-sp-1.govt.nz/realm/samlapp1</wsa:Address>
               </wsa:EndpointReference>
            </wsp:AppliesTo>
            <wst:RequestedAttachedReference>
               <wsse:SecurityTokenReference TokenType="http://docs.oasis-
open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0">
                  <wsse:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-
wss-saml-token-profile-1.1#SAMLID">b7332bb4143c5d6e60fcad032df92e58</wsse:KeyIdentifier>
               </wsse:SecurityTokenReference>
            </wst:RequestedAttachedReference>
            <wst:Lifetime>
               <wsu:Created>2010-09-23T22:36:47Z</wsu:Created>
               <wsu:Expires>2010-09-23T22:51:47Z</wsu:Expires>
            </wst:Lifetime>
         </wst:RequestSecurityTokenResponse>
      </wst:RequestSecurityTokenResponseCollection>
   </env:Body>
</env:Envelope>
```

6. The Redeem Token Request

The Redeem Token Request contains a message providing an opaque token that was issued to a source Service Provider and subsequently passed to a target service provider. The target Service Provider can pass the opaque token to the Context Mapping Service in a Redeem Token Request message, which will ensure that the token is valid, the user account is in a valid state, the opaque token had been issued for the target Service Provider, and will translate the opaque token into a SAML 2.0 token that provides identity information to the target Service Provider in a form it can use. This corresponds to step 4 in section 8 of this document.

6.1 Protocol

The value of the WS-Addressing Action header MUST be http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Validate. The root element contained in the SOAP body MUST be a **RequestSecurityToken** message. This specification does not allow for batch validation.

This is described in [ws-trust-1.3] §7.

6.2 Message Elements

Element <RequestSecurityToken>

This message will contain the following elements and attributes:

Attribute / Element	WS-Trust v1.4 Requirement	Context Mapping Service Requirement
Context	MAY be provided.	As per WS-Trust v1.3 requirement.
TokenType	MAY be provided.	MUST be provided. The value MUST be http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0.
RequestType	MUST be provided and contain the value of . 'http://docs.oasis-open.org/ws-sx/ws-trust/200512 /Validate'	As per WS-Trust v1.3 requirement.
ValidateTarget	MUST be provided.	As per WS-Trust v1.3 requirement. The content SHALL be the opaque token that the source Service Provider passed to the target Service Provider.

Attribute / Element	WS-Trust v1.4 Requirement	Context Mapping Service Requirement
AllowCreateFLT	Not Applicable.	This is an extension element to the request defined by this specification. It MAY be provided. If it absent, then the Context Mapping Service will require that the user be registered with the target Service Provider and will return a status of invalid. If this element is present, then the Context Mapping Service will create a registration, assign a new FLT, and return the new FLT. This element is defined in the namespace `urn:nzl:govt:ict:stds:authn:deployment:igovt:gls:sts:1_0`

6.3 Sample Request

The following is a sample Validate Token Request message:

```
<env:Envelope>
   <env:Header>
      <wsa:Action>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Validate</wsa:Action>
      <wsse:Security>
         <!-- ... -->
      </wsse:Security>
   </env:Header>
   <env:Body>
      <wst:RequestSecurityToken>
         <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</wst:TokenType>
         <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Validate</wst:RequestType>
         <wst:ValidateTarget>
            <saml2:Assertion IssueInstant="2010-09-23T22:36:47Z"
ID="b7332bb4143c5d6e60fcad032df92e58" Version="2.0">
               <!-- ... -->
            </saml2:Assertion>
         </wst:ValidateTarget>
         <iCMS:AllowCreateFLT />
      </wst:RequestSecurityToken>
   </env:Body>
</env:Envelope>
```

7. The Redeem Token Response

The Redeem Token Response contains a message providing a token to the target Service Provider. The token can be used by the target Service Provider; the SPNameQualifier attribute of the NameID element identifies the target Service Provider. The user's FLT for the target Service Provider is contained in the returned token. The token can be used in Opaque Token Request message so that the target Service Provider may act as a source Service Provider for another target Service Provider. This corresponds to step 5 in section 8 of this document.

7.1 Protocol Binding

The value of the WS-Addressing Action header MUST be http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTR/ValidateFinal. The root element contained in the SOAP body of a successful response from MUST be a single **RequestSecurityTokenResponseCollection** element. Negotiation or multi-leg authentication is not supported.

7.2 Message Elements

Element <RequestSecurityTokenResponse>

This message will contain the following elements and attributes:

Attribute / Element	WS-Trust v1.4 Requirement	Context Mapping Service Requirement
Context	MAY be provided, but if the corresponding RequestSecurityToken element provided a value for Context, then it MUST be echoed here.	As per WS-Trust v1.3 requirement.
TokenType	MAY be provided.	MUST be provided. MUST be http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0.
RequestedSecurityToken	MUST be provided	As per WS-Trust v1.3 requirement. This content of this element SHALL be a SAML 2.0 assertion that is compatible with the assertions generated by the igovt logon service Web SSO. Refer to [ils-saml20-1.6.5] for details. However, since the interaction will be with a service acting for the end user rather than the user, the subject confirmation method SHALL be `urn:oasis:names:tc:SAML:2.0:cm:sender-vouches`.
Status	MUST be provided	As per WS-Trust v1.3 requirement.

Attribute / Element	WS-Trust v1.4 Requirement	Context Mapping Service Requirement
Status/Code	MUST be provided.	As per WS-Trust v1.3 requirement. MUST be either http://docs.oasis-open.org/ws-sx/ws-trust/200512/status/valid or http://docs.oasis-open.org/ws-sx/ws-trust/200512/status/invalid.
Status/Reason	MAY be provided.	As per WS-Trust v1.3 requirement.

7.3 Sample Response

The following is a sample Validate Token Response message:

```
<env:Envelope>
   <env:Header>
      <wsa:Action>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RSTR/ValidateFinal</wsa:Action>
      <wsse:Security>
         <!-- ... -->
      </wsse:Security>
   </env:Header>
   <env:Body>
      <wst:RequestSecurityTokenResponse>
         <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</wst:TokenType>
         <wst:RequestedSecurityToken>
            <saml2:Assertion IssueInstant="2010-09-23T22:36:56Z"
ID="c5d6e602df92e58fcad03b7332bb4143" Version="2.0">
               <saml2:Issuer>https://www.i.govt.nz/sts</saml2:Issuer>
               <!-- ... -->
            </saml2:Assertion>
         </wst:RequestedSecurityToken>
         <wst:Status>
            <wst:Code>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/status/valid</wst:Code>
         </wst:Status>
      </wst:RequestSecurityTokenResponse>
   </env:Body>
</env:Envelope>
```

8. Context Mapping Service Messaging Flow

The following sequence diagram describes the messaging flow for a source Service Provider invoking an operation at a target Service Provider, and the Context Mapping Service being used to exchange the user's identity in a manner that prevents the Service Providers establishing a common identifier for the user.

Not shown in this diagram is the action that initiates this message flow. There are two possible actions. Either the user establishes an interactive web session with the source Service Provider and performs some action that causes the source Service Provider to invoke an operation of the target Service Provider, or the Source Agency is responding to such an invocation from another source Service Provider, and in turn is invoking an operation at another target Service provider.

The diagram only shows the main processing flow, where requests are processed successfully. No exceptional flow is shown.

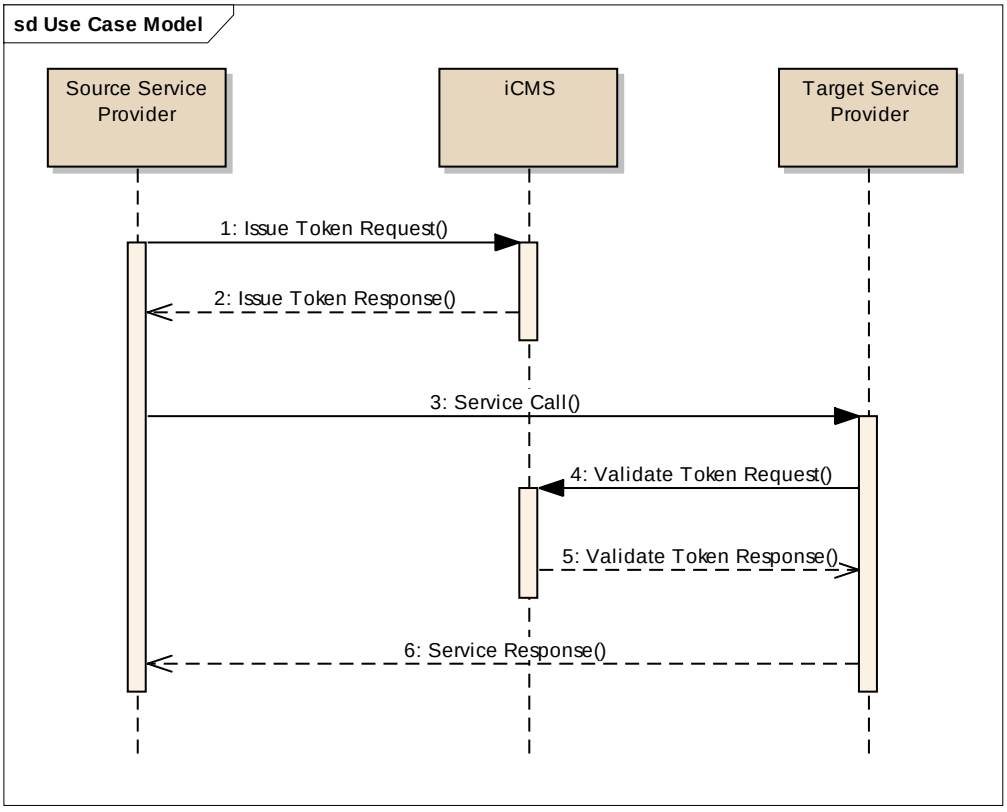

Figure 1 – Authentication Messaging Sequence Diagram

Message	Description
1. Opaque Token Request	The source Service Provider has determined that it needs to invoke an operation at a target Service Provider, and makes a request to the Context Mapping Service to provide a token that can be passed to the target Service Provider. The request will identify both the user that is the subject of the request, and the target Service Provider that will be invoked. The source Service provider may state the lifetime that it would like the returned token to be valid for.

Message	Description
2. Opaque Token Response	The Context Mapping Service performs required validation of the use's igovt logon account and returns an opaque token. The token is a SAML 2.0 Assertion but must be considered opaque by the source Service Provider. The response returns the token itself, and XML fragments that can be used verbatim as a WS-Security SecurityTokenReference for the token when it is attached to the message from the source Service Provider to the target Service Provider. The valid lifetime of the token is encoded into the token itself, but the source Service Provider MUST NOT attempt to use this information. Instead, the Issue Token Response repeats the valid lifetime information in the WS-Trust information for the source Service Provider to make use of. The returned valid lifetime values MAY be different to any value that was requested. The Context Mapping Service will be configured with policy to provide default values and limitations on the values that can be returned.
3. Service Call	This is the service call from the source Service Provider to the target Service Provider. Other than that the token in the Issue Token Response must be passed to the target Service Provider, this messaging specification makes no constraints on the service call.
4. Redeem Token Request	The target Service Provider has received an opaque security token in a request message from the source Service Provider. The target Service Provider MUST NOT attempt to parse or understand this token, but must include it in a Validate Token Request to the Context Mapping Service.
5. Redeem Token Response	The Context Mapping Service processes the token that it created for the Issue Token Response. It performs required validation of the user's igovt logon account. It confirms that the target Service Provider making the request is the same Service Provider identified in the opaque token, which is the same provider that the source Service Provider nominated in the Issue Token Request. If all checks are passed, the Context Mapping Service creates and returns a SAML 2.0 token, which the target Service Provider may understand and process.
6. Service Response	The target Service Provider completes processing for the source Service Provider. The details of this are excluded from this specification.

9. Fault Codes

The fault messages returned by the igovt Context Mapping Service are standard SOAP 1.2 faults. This section defines the error sub-codes in the namespace `urn:nzl:govt:ict:stds:authn:deployment:igovt:gls:iCMS:1_0`. The table identifies the sub-codes with local names only. Where sub-codes are further broken down into more detailed sub-codes, this will be written as <more general sub-code>/<more detailed sub-code>. This section only describes the faults that are specific to the igovt logon service STS, and is not an exhaustive list of all faults that could be raised. Only sender faults have sub-codes. Receiver faults indicate unexpected processing errors for the igovt logon service STS.

The Reason element of the fault messages will contain text that is suitable for recording in application logs to aid with problem resolution.

9.1 Sender Sub-codes

The following table enumerates the SOAP fault sub-codes that the Context Mapping Service will provide for the Sender.code

Sub-code	Scenario
InvalidConsentValue	The value of the user's consent, as contained in the Claims element of the Issue Token Request, was not current-explicit.
InvalidAgencyCertificate	The agency messaging certificate used to sign the SOAP request message does not match the certificate configured in the igovt logon service STS for the agency identified as the audience of the token in the request.
InvalidEntityID	The entity ID supplied as the target service agency ID in the AppliesTo element of the issue request does not match a service agency known to the igovt logon service STS.
InvalidTokenType	The requester supplied a value for TokenType that was not http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0.
ValidityPeriodPreDated	The requested lifetime in an Issue Token request was specified with a created time too far in the past.
ValidityPeriodPostDated	The requested lifetime in an Issue Token request was for a period of time in the future. The igovt logon service will only issue tokens that are immediately current.
ValidityPeriodReversed	The requested lifetime in an Issue Token request period has a created time set to later than the expires time.
InvalidAction	The WS-Address Action header was not a legal value for the RequestType supplied in the message body.
ExpiredToken/UserAuthentication	The lifetime of the token included in the Token Issue Request has expired.
ExpiredToken/Opaque	The lifetime of the token included in the Token Validate Request has expired.
InvalidToken/MissingToken	There was no token supplied in the request; either the ActAs token of the Issue Token Request, or the ValidateTarget of the Validate Token Request.

Sub-code	Scenario
InvalidToken/MissingIdentifier	The supplied authentication token was missing a NameID or EncryptedID element. This indicates a problem with the tokens issued by the igovt logon service.
InvalidToken/Unparsable	The XML structure of the authentication tokens was broken in some way that prevented normal processing. This may indicate a problem with the tokens issued by the igovt logon service. It also may indicate that the service agency is altering the tokens before passing to the igovt logon service in a request message.
InvalidToken/InvalidAudiences	The token was presented to service not listed in the audience restriction. This indicates either presenting opaque tokens to the opaque token service or other token types to the redeem token service.
InvalidToken/Signature/Missing	The supplied SAML 2.0 token was missing a signature element. This indicates a problem with the tokens issued by the igovt logon service.
InvalidToken/Signature/Profile	The supplied SAML 2.0 token had signature element that did not conform to the profile specified by [saml-core-2.0-os]. This indicates a problem with the tokens issued by the igovt logon service.
InvalidToken/Signature/Invalid	The supplied SAML 2.0 token had signature element that could not be validated. This may indicate a problem with the tokens issued by the igovt logon service. It also may indicate that the service agency is altering the tokens before passing to the igovt logon service in a request message.
InvalidToken/InvalidTokenSubType	The token subtype in the opaque token request was either missing, or was not one of the three values listed in section 4.2.
Logon/NotFound	No record could be found for the igovt logon identified by the token in the request message.
Logon/Suspended	The logon identified by the token in the request has been suspended.
Logon/NoFLTForTargetAgency	The logon is not registered with the target agency. This fault will not be raised by the Issue Token Request. It is only raised by the Validate Token Request if the target agency has not supplied the AllowCreate flag.