RealMe

SAML v2.0 Messaging Introduction

Version: 1.0 – APPROVED

Author: Richard Bergquist
Datacom Systems
(Wellington) Ltd

Date: 15 November 2012

Table of Contents

1 Introduction

1.1 Document Purpose

RealMe exposes a SAML v2.0 interface to integrating Client organisations which conforms to the New Zealand Security Assertion Messaging Standard (NZ SAMS).

This document introduces the SAML v2.0 interfaces and presents information that is common across them.

1.2 Document Map

The RealMe Messaging specifications contain their own document map to the child documents that are referenced.

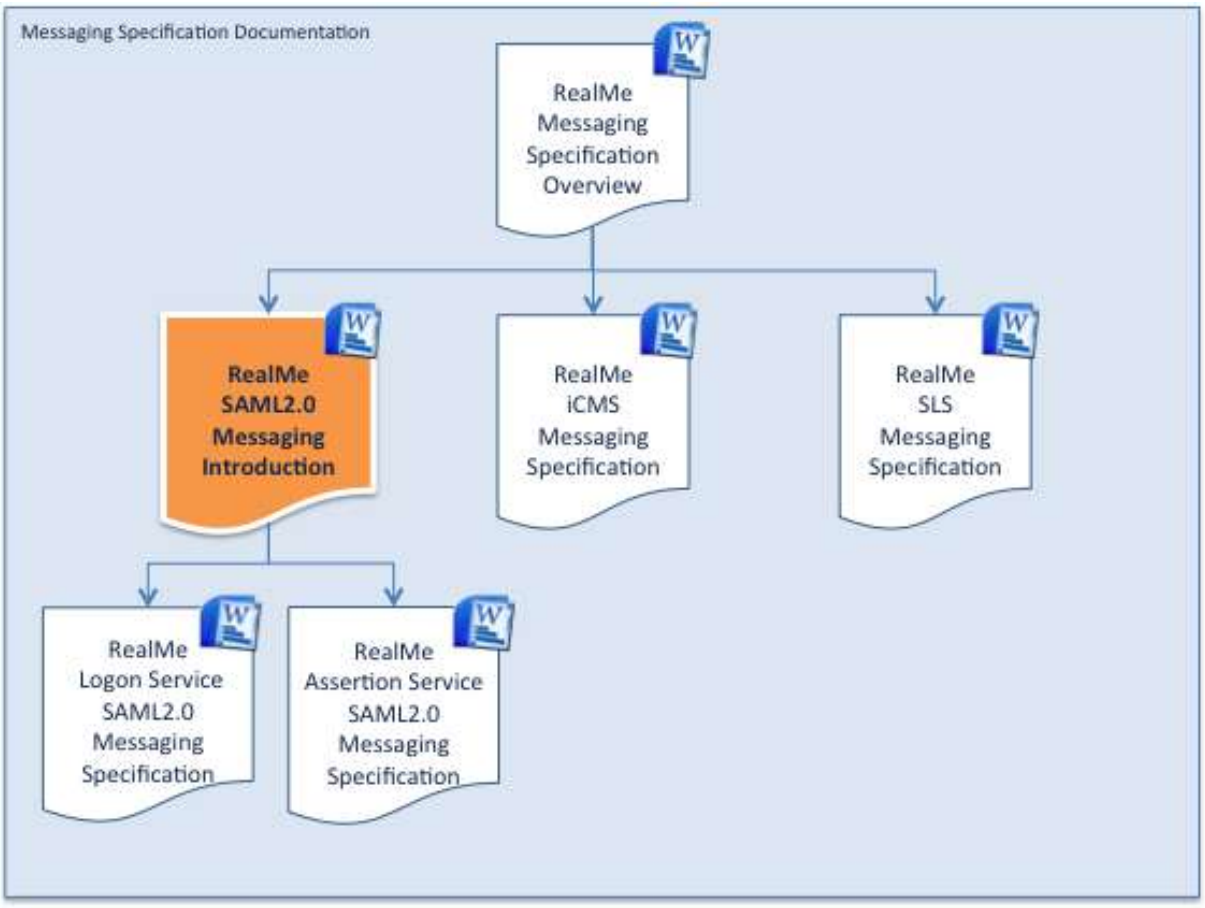

Figure 1 – RealMe Message Specification Document Map

1.3 The SAML v2.0 Interfaces

RealMe contains the following SAML v2.0 interfaces:

SAML v2.0 Interface	Document Reference	Description
The RealMe Logon Service	[realme-logon-saml-spec].	A SAML v2.0 interface for providing an authentication service for Customers of RealMe integrated Clients
The RealMe Assertion Service	[realme-assert-saml-spec]	A SAML v2.0 interface for providing an identity assertion service for Customers of RealMe integrated Clients/

Table 1 – Types of RealMe SAML v2.0 Interfaces

Each of the interfaces are fully described in the referenced document.

2 Messaging Overview

RealMe exposes a SAML v2.0 interface for Service Provider's to interact with RealMe.

The Security Assertion Markup Language (SAML) is a specification by OASIS that defines the syntax and processing semantics of assertions made about a subject by a system entity. In the course of making, or relying upon such assertions, SAML system entities use defined protocols to communicate either regarding an assertion itself, or the subject of an assertion. This specification defines both the structure of SAML assertions, and an associated set of protocols, in addition to the processing rules involved in managing a SAML system.

The SAML v2.0 specification is broad in scope. The NZ SAMS is a NZ government agency deployment profile of the SAML v2.0 standard and prescribes the design and transport of SAML v2.0 messages with NZ government online services. Together, these standards present a number of mechanisms to fulfil several federated identity management objectives.

These objectives are broadly termed 'profiles' and are covered in reference [saml-profiles-2.0-os] and are constrained by NZ SAMS.

Within each profile the specification further describes how SAML v2.0 can be used to achieve the required objective. Options here concern:

1. The message protocols used. The document reference [saml-core-2.0-os] defines these and NZ SAMS further constrains the protocols used.
2. Precisely which message elements from the SAML v2.0 request and response are required to be used. The document reference [saml-core-2.0-os] defines these and NZ SAMS further constrains the elements used.
3. The SAML v2.0 bindings used to convey these messages. The document reference [saml-bindings-2.0-os] defines these options and NZ SAMS further constrains the bindings used.
4. Signing and encryption options used in the messages.
5. Security implications of options chosen.

The finer grained options chosen here are also termed part of the chosen SAML v2.0 profile.

2.1 Scope

The profile implemented is the SP-initiated **'Web Browser SSO Profile'** from section 4.1 of [saml-profiles-2.0-os].

Explicitly, it SHALL NOT include the profiles in [saml-profiles-2.0-os] of:

1. Enhanced Client or Proxy (ECP) Profile (section 4.2)

2. Identity Provider Discovery Profile (section 4.3)
3. Single Logout Profile (section 4.4)
4. Name Identifier Management Profile (section 4.5)
5. Assertion Query/Request Profile (section 6)
6. Name Identifier Mapping Profile (section 7)

2.2 Bindings Overview

The specifications will define the use of:

1. The HTTP-Redirect binding over HTTPS for the request by the SP.
2. The HTTP-Artifact binding over HTTPS for sending a SAML assertion by RealMe IdP. This applies to both “SP Initiated SSO” and “IdP Initiated SSO”.

2.3 Messaging Pre-Requisites

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

2.3.1 Provide RealMe with the SP SAML v2.0 Metadata.

Each SP MUST provide RealMe Operations Manager with the SP’s SAML v2.0 metadata. The SAML v2.0 specification describes the use of metadata in [saml-metadata-2.0-os] and is constrained by NZ SAMS Section 9.

SAML v2.0 metadata is used to contain agreements between system entities regarding identifiers, binding support and endpoints, certificates and keys, and so forth. The metadata specification is useful for describing this information in a standardised way.

The SP’s SAML v2.0 messaging public key certificate(s) MUST be included in the exchanged metadata. The certificate(s) will be extracted and introduced into RealMe’s PKI. See 2.3.3 for use of dual certificates.

This process includes the usage agreement of the set of information from the RealMe Identity Attribute Providers. It requires an out-of-band integration step between trusted parties. All SP SAML v2.0 implementations MUST support the production and consumption of metadata as described in [saml-metadata-2.0-os].

2.3.2 Receive RealMe SAML v2.0 Metadata

RealMe SHALL supply the SP with its SAML v2.0 metadata for the SP to load into their SAML v2.0 provider. The SAML v2.0 specification describes the use of metadata in [saml-metadata-2.0-os] and is constrained by NZ SAMS Section 9. This process will be the reciprocal process step to 2.3.1, and SHALL include RealMe ’s SAML v2.0 messaging public key certificate(s).

RealMe’s metadata MUST be used to extract RealMe’s SAML v2.0 messaging public key certificate(s) into the SP’s PKI.

2.3.3 SAML Messaging Certificates.

It MAY be possible to have distinct certificates for message signing and encryption. This specification SHALL only require a sole signing certificate and this MUST be present in the SP metadata. If message encryption is also used then this MUST be present in the SP metadata.

The SAML v2.0 specification describes messaging certificates in metadata in the [saml-metadata-2.0-os] and is constrained by NZ SAMS section 9.

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

2.3.4 Web Server SSL Certificates

Each SP MUST use a SAML v2.0 implementation that is only accessible over HTTPS. The connection MUST be configured with certificates signed by a publically trusted Certificate Authority. This is REQUIRED to allow the user's browser to interact securely with the SP's SAML endpoints.

Note that while SSL certificates are used, they are not conveyed in the metadata. Refer to NZ SAMS page 57 for more information.

2.3.5 Mutual SSL Certificates

Mutual SSL will be used to convey the SAML response over SOAP via the SAML HTTP-Artifact binding. The SP MUST provide the RealMe Operations Manager with their client certificate and RealMe SHALL provide each SP with RealMe server certificate for this exchange.

Note that while SSL certificates are used, they are not conveyed in the metadata. Refer to NZ SAMS page 57 for more information.

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

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

2.3.6 Server Synchronisation

The SP's server's system clock MUST be closely synchronised with a New Zealand Stratum One NTP Time Server.

This is REQURIED in order to:

1. Ensure the limited life time of the sender's message is not exceeded due to system time variations.
2. Ensure assertions are honoured within a timeframe that is in common with the Client SP and RealMe IdP.

Time tolerances in RealMe MAY be subject to change. Indicative tolerance values are +/- 1 minute for item 1 and up to 10 minutes for item 2.

It is RECOMMENDED that a NTP service be installed locally within an integrators infrastructure to meet this requirement.

Refer to http://www.ntp.org for strategies on how to implement time synchronisation from a NTP time server.

Refer to NZ e-GIF where UTC (MSL) is the Stratum One NTP time server, with NTP v4 as the delivery method over the internet.

2.4 Conventions

2.4.1 Conformance Annotations

The specifications describes the SAML v2.0 messaging elements used and their conformance or constraint to parent standards.

The following convention is used to annotate conformance or constraints in the specifications.

[1] This will conform with [NZISM].

Annotation	Interpretation
SAML v2.0	Conforms to OASIS SAML v2.0 standard.
NZ SAMS	Conforms to NZ SAMS.
SAML v2.0	Constrains OASIS SAML v2.0 standard.
NZ SAMS	Constrains NZ SAMS.

Table 2 - Conformance Annotations

2.4.2 XML Structures

The follow convention is used to distinguish between XML attributes and XML elements in the SAML v2.0 messaging.

Structure	Representation
Attribute	AttributeName
Element	<ElementName>

Table 3 - XML Structure Conventions

END

REALME SAML V2.0 MESSAGING INTRODUCTION.