RealMe®

Technical Overview: November 2013

Venkat Maddali
Solution Architect
Department of Internal Affairs
What is RealMe?

RealMe is a partnership between New Zealand Post and Department of Internal Affairs.

RealMe offers:

- **Authentication: RealMe Login Service**
  The RealMe Login Service allows the user to use a same login (i.e. username and password) to access a wide range of public and private sector online services.

- **Online Identity Assurance: RealMe Assertion Service**
  The RealMe Assertion Service allows the user to provide their verified personal information from multiple authoritative source to a wide range of private and public sector online services.
Key Terminology

- **RealMe Account** – also known as RealMe login which allows the user to authenticate at the relying parties. The user can create multiple accounts and they are pseudonymous.

- **RealMe Verified Account** – the user can have only one verified account which can be accessed via moderate strength authentication (username, password and OTP). The verified account is linked with verified identity (IVS) and verified residential address (AVS) through user consent.
RealMe Services – Current State

Client organisations

- Agencies
- Banks

Launch market focus

Powered by

RealMe login – low or moderate

Platform Applications

- ID Assurance

Consent Service

Account Service

Personal Information Providers

- NZP
- DIA
RealMe Key Principles

The following are few key principles for RealMe

• Privacy
• User centricity
• Integrity
• Security
RealMe Integration Patterns

- Login Integration Patterns (RealMe <-> RP)
- IAP Integration Patterns (RealMe <-> IAP)
- Identity Assurance Integration Patterns (RealMe <-> RP)
Login Integration Patterns

- Login Only – core user authentication pattern
- Extend Login – an extension to Login Only integration pattern
- Seamless Login - an extension to Login Only integration pattern
Login Integration Patterns
L1 – Login Only

Relying Party Context:

- Relying Party is required to authenticate a user for
  - Account creation
  - Apply for entitlements
  - Identifying the user returning to the service, etc

- The relying party runs their own evidence of identity (EOI) process to verify the user and granting entitlements etc
Login Integration Patterns
L1 – Login Only

1. Initiates transaction
2. forwards
3. SAMLv2.0 Authn Request
4. Displays login page and user submits credentials
5. SAMLv2.0 Artifact
6. Artifact Resolve
7. SAML v2.0 Assertion
8. FLT + Authentication strength
9. Landing Page
Login Integration Patterns

L1 – Login Only

High Level Use Case Diagram

- User submits credentials
- RealMe creates login
- Login
- User provisioning
- Entitlement management
- Relying party applies
Login Integration Patterns
L1 – Login Only

Technical Integration Specification

Login Integration Standard: SAMLv2.0

- Profile: Web SSO Profile – SP initiated SSO
- Binding: Artifact Binding
Login Integration Patterns
L2 – Extend Login

Relying Party Context:

Relying Party extends the user authentication to other relying parties (web services) to:

- pull personal information to support their EOI process, entitlement process, etc
- push personal information to support other relying party's EOI process, entitlement process
Login Integration Patterns

L2 – Extend Login

10. Submits details
11. Request Token for RP2
12. Encrypted SAML Token
13. Request for personal info
14. Decrypt SAML Token
15. SAML Token with FLT$_{RP2}$
16. Response
17. Confirmation message
Login Integration Patterns
L2 – Extend Login

High Level Use Case Diagram

- RealMe
  - Login
  - Extend Login Context
- User Provisioning
- Relying Party
  - Include
  - Include
- Relying Party 2
  - Send / Update Personal Information

User Submits credentials
Apply

<<include>>
<<include>>
<<include>>
<<extend>>
Login Integration Patterns
L2 – Extend Login

Technical Integration Specification

Integration Standards: SAMLv2.0, WS-Trust 1.4

- SAMLv2.0 Profile: Web SSO Profile – SP initiated SSO
- SAMLv2.0 Binding: Artifact Binding
- WS-Trust Bindings: Issue and Validate
Login Integration Patterns

L3 – Seamless Login

Relying Party Context:

• Two relying parties have a direct relationship and one relying party provides a navigational link, so that the user can seamlessly navigate to other relying party to:

  • View/ manage their account at the other relying party
  • Apply for entitlements, etc
Login Integration Patterns

L3 – Seamless Login

10. Clicks Link to RP2

11. Request Token for seamless login to RP2

12. Encrypted SAML Token

13. Redirect with token

14. SAMLv2.0 Assertion through Artifact Binding (IDP initiated SSO)

15. Authn strength

+ FLT²

16. Landing Page

User

Relying Party

Web Application

SAMLv2.0 Service Provider

Relying Party2

Login Service (SAMLv2.0 IDP)

Context Mapping Service (STS)
Login Integration Patterns
L3 – Seamless Login

Technical Integration Specification

Integration Standard: SAMLv2.0, WS-Trust 1.4

- SAMLv2.0 Profile for RP2: Web SSO Profile – IDP initiated SSO
- SAMLv2.0 Binding for RP2: Artifact Binding
- WS-Trust Bindings for RP1: Issue
Login Integration Patterns
L3 – Seamless Login

High Level Use Case Diagram

RealMe

Login
Seamless Login

User

Submits credentials
Manages

Relying Party

<<include>>
Manage Account
<<extend>>

<<include>>

Manage Account

<<include>>

Navigate to RP2

Relying Party 2

Create/Manage Account

<<include>>

New Zealand Post

INTERNAL AFFAIRS
Te Tari Taiwhenua
RealMe Verified Account

- The RealMe Verified Account is like a dashboard for the user.
- RealMe doesn’t store any personal information, rather collates the personal information from the identity attribute providers and displays them to the user.
- The user can see the account information from the Identity Attribute Provider, which includes the status (No Account, In Progress, Valid, and Invalid) and the personal information if the status is “valid”.
- RealMe also provides navigational links to the identity attribute providers so that the user can apply for an account or update their account at the identity attribute providers.
IAP Integration Patterns

- Get Status or Personal information – retrieving status or personal information from identity attribute provider

- Seamless Login to Identity Attribute Provider - is an implementation of seamless login use case (i.e. navigating the user from RealMe to identity attribute provider seamlessly).
IAP Integration Patterns

IAP1 – Get Status or Personal Information

1. Clicks Manage Verified Account
2. SAML Authn Request
3. moderate strength authentication
4. SAML Assertion
5. Provides consent for RealMe
6. Notify Consent: Service issues consent token
7. Get Token for IVS or AVS
8. Encrypted SAML Token
9. SAML Attribute Query Request
10. Decrypt SAML Token. Returns FLT\textsubscript{iap}
11. SAML Attribute Query Response
12. Display personal information

Consent Service
Context Mapping Service (STS)

Login Service (SAMLv2.0 IDP)
Account Service (SAMLv2.0 SP)

Identity Attribute Providers
IVS
AVS
IAP 3
IAP 4
Web Bank
IAP Integration Patterns
IAP1 – Get Status or Personal Information

Technical Integration Specification

Integration Standards for IAP: SAMLv2.0, WS-Trust1.4

- SAMLv2.0 Profile: Attribute Query Profile
- SAMLv2.0 Binding: SOAP Binding
- WS-Trust1.4 Bindings – Validate
IAP Integration Patterns

IAP2 – Seamless Login to IAP

12. Clicks Apply Button to IVS

13. Get Token for IVS

14. Encrypted SAML Token

15. Redirect with token

16. SAML Assertion (IDP initiated SSO)

17. Landing Page

Login Service (SAMLv2.0 IDP)

Account Service (SAMLv2.0 SP)

Context Mapping Service (STS)

RealMe

Identity Attribute Providers

IVS

AVS

Agency 3

Agency 4

Web Bank
IAP Integration Patterns
IAP2 – Seamless Login to IAP

Technical Integration Specification

Integration Standards for IAP: SAMLv2.0

- SAMLv2.0 Profile: WebSSO Profile – IDP initiated SSO
- SAMLv2.0 Binding: Artifact Binding
Identity Assurance integration patterns
A1 – Assert only

Relying Party Context:

• The user is required to provide verified personal information to the Relying Party online:
  • For account creation (e.g. at a bank)
  • Apply for an Entitlement (e.g. for a student loan, mortgage etc)

• The Relying Party wants to reduce their back office process for the verification of user provided data.
Identity Assurance integration patterns
A1 – Assert only

1. Initiates transaction
2. forwards request
3. SAML Authn Request
4. SAML Authn Request
5. Username + password
6. SAML Assertion
7. Check Consent
8. Token for IVS/AVS
9. Encrypted Token
10. SAML Attribute Query Request
11. Decrypt Token. Returns FLT<sub>IVS</sub>
12. Provides consent to displayed data
13. SAML Assertion Through artifact binding
14. Returns personal info
15. Confirmation page
Identity Assurance integration patterns
A1 – Assert only

Technical Integration Specification

Assertion Integration Standard: SAMLv2.0

- Profile: Web SSO Profile – SP initiated SSO
- Binding: Artifact Binding
Few other points

- Mature integration process and detailed integration collateral

- RealMe exposes multiple integration environments for the relying parties
  - Dev to RealMe MTS
  - Test to RealMe ITE
  - Production/ DR to RealMe production

- RealMe services can be extended to mobile applications as the user interface follows the responsive design.
Questions ???