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**

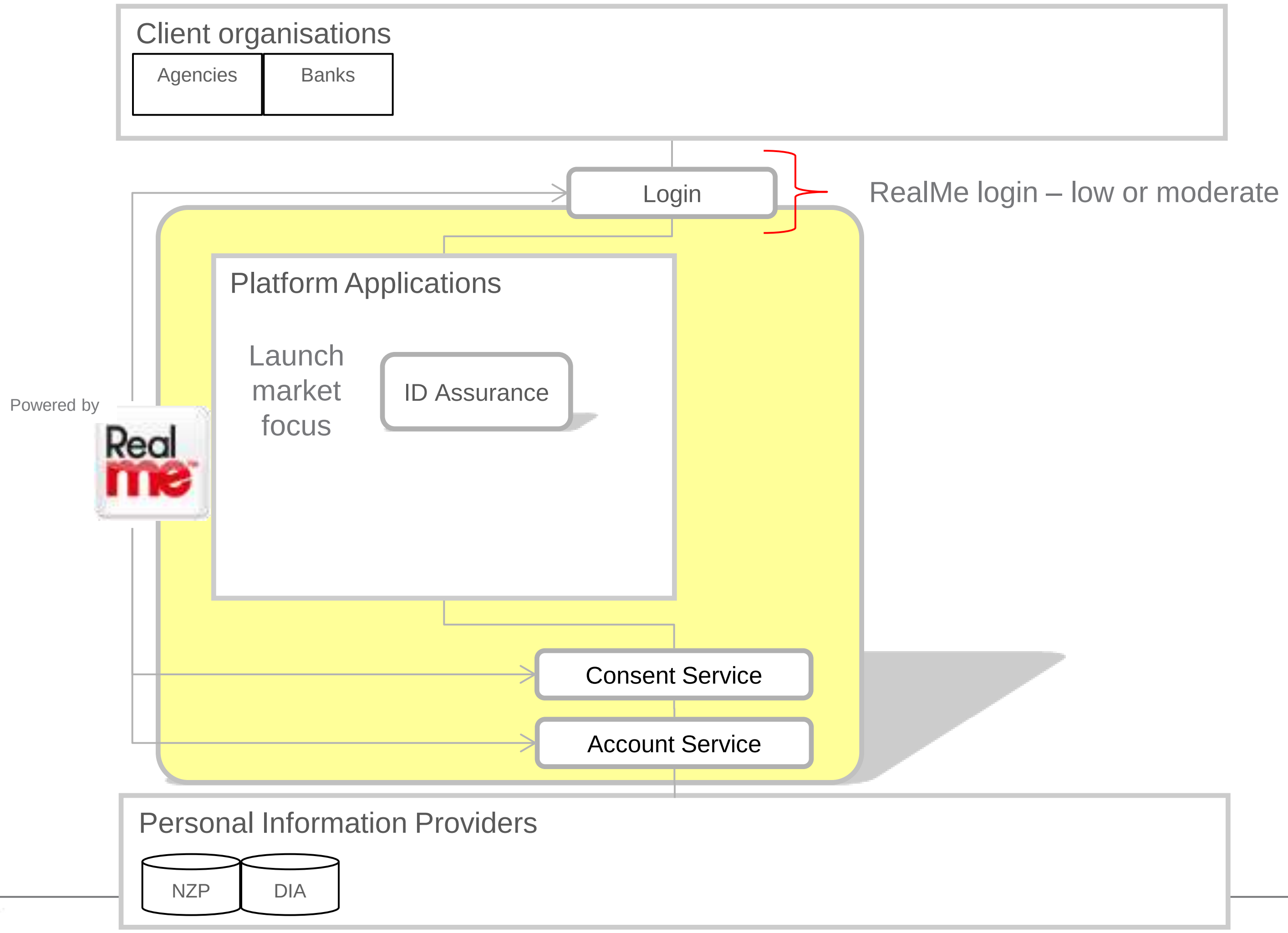
  The RealMe Assertion Service allows the user to provide their verified personal information from multiple authoritative source to a wide range of private and public sector online services.

Key Terminology

- **RealMe Account** – also know 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



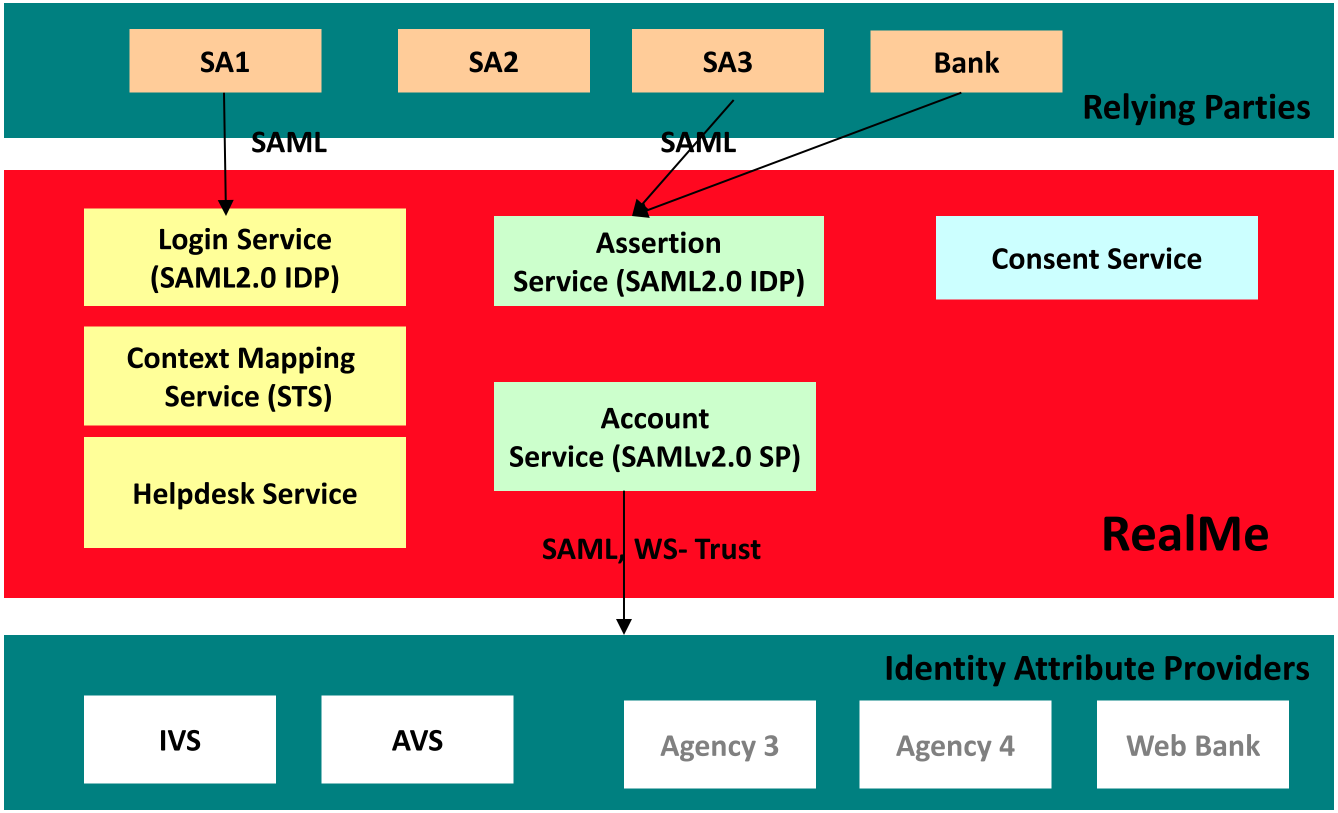
RealMe Key Principles

The following are few key principles for RealMe

- **Privacy**
- **User centricity**
- **Integrity**
- **Security**

.

RealMe ecosystem


SA1
SA2
SA3
Bank
Relying Parties
SAML
SAML
Login Service (SAML2.0 IDP)
Assertion Service (SAML2.0 IDP)
Consent Service
Context Mapping Service (STS)
Account Service (SAMLv2.0 SP)
Helpdesk Service
SAML, WS- Trust
RealMe
Identity Attribute Providers
IVS
AVS
Agency 3
Agency 4
Web Bank

INTERNAL AFFAIRS
Te Tari Taiwhenua

New Zealand Post

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

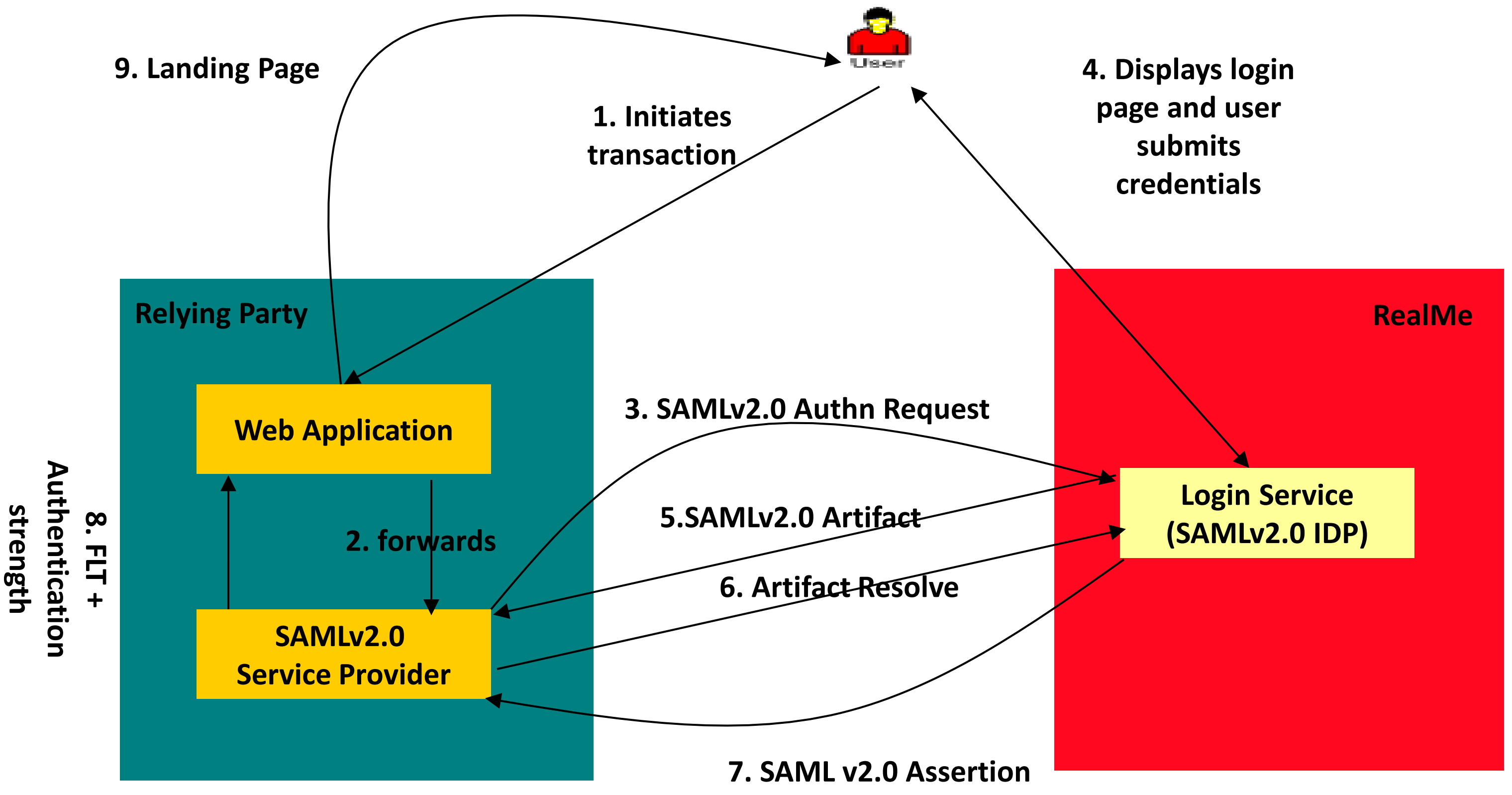
L1 – Login Only

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

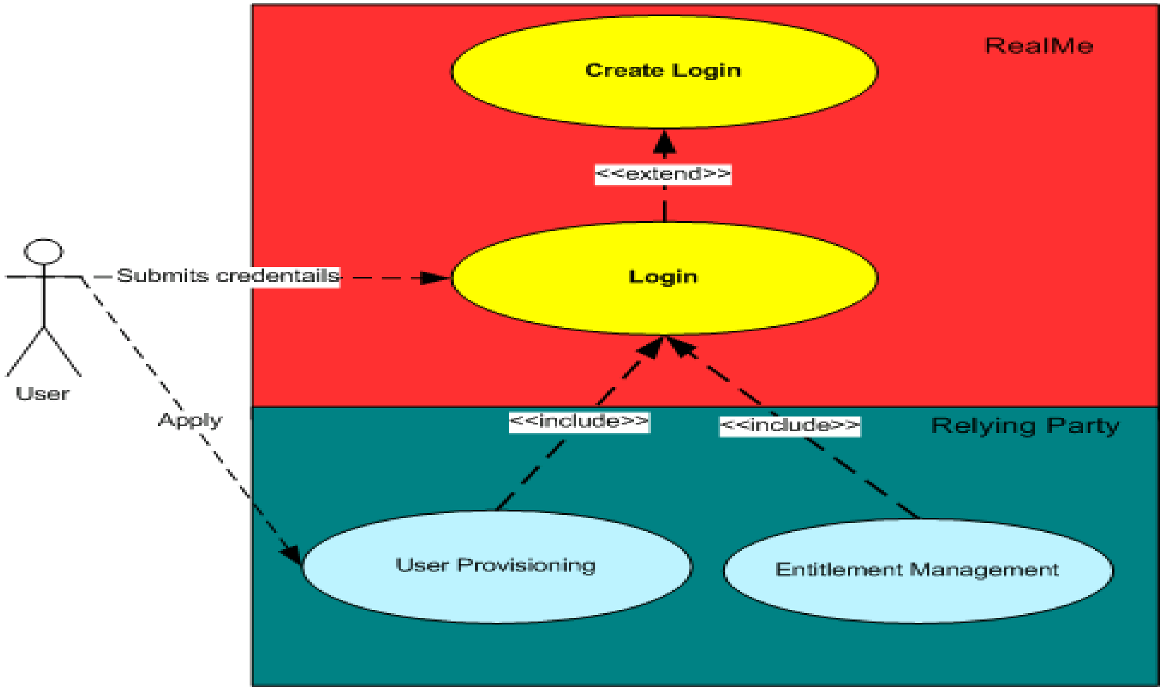
L1 – Login Only


User
9. Landing Page
1. Initiates transaction
4. Displays login page and user submits credentials
Relying Party
RealMe
Web Application
3. SAMLv2.0 Authn Request
Login Service (SAMLv2.0 IDP)
5.SAMLv2.0 Artifact
2. forwards
8. FLT + Authentication strength
6. Artifact Resolve
SAMLv2.0 Service Provider
7. SAML v2.0 Assertion

Login Integration Patterns

L1 – Login Only

High Level Use Case Diagram



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

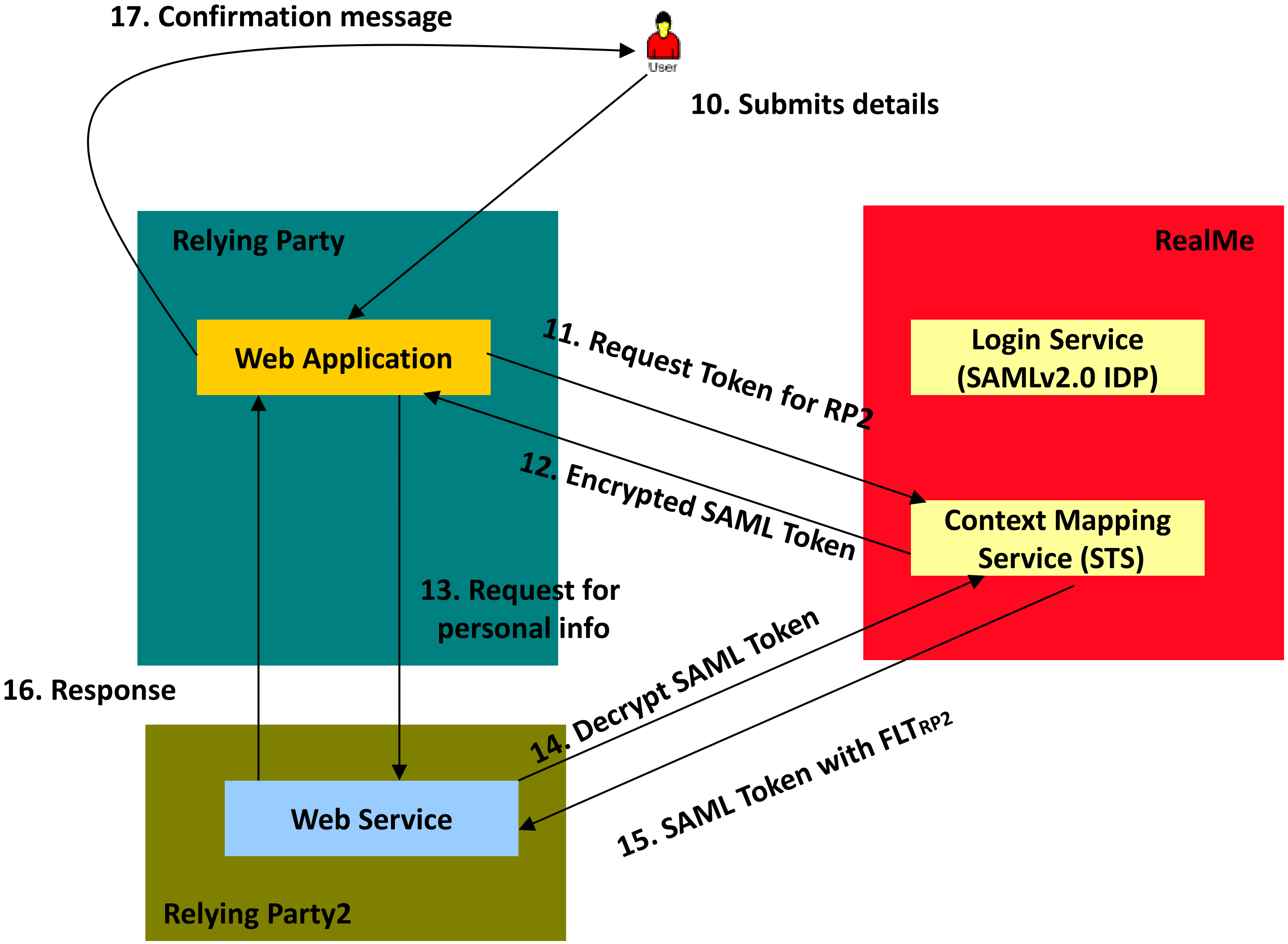
Relying Party Context:

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

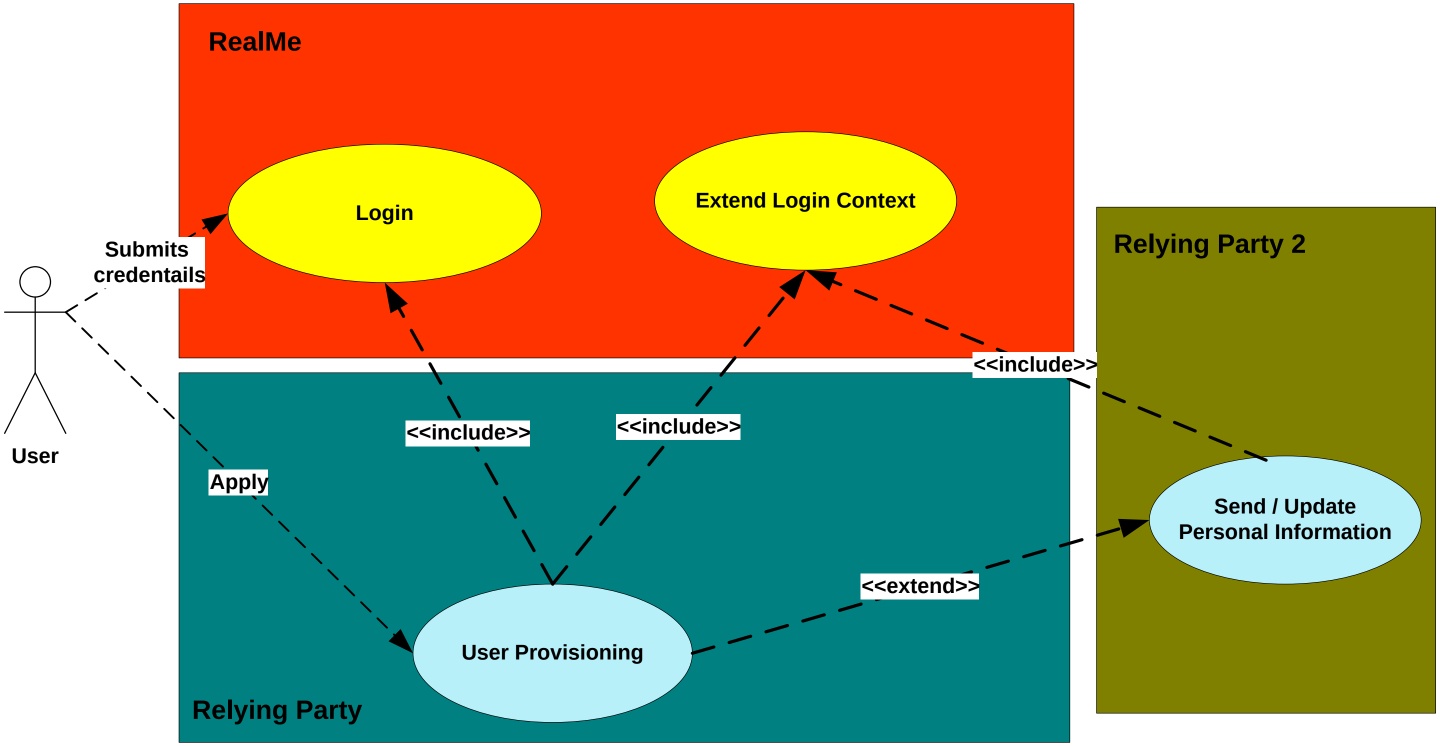
L2 – Extend Login



Login Integration Patterns

L2 – Extend Login

High Level Use Case Diagram



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

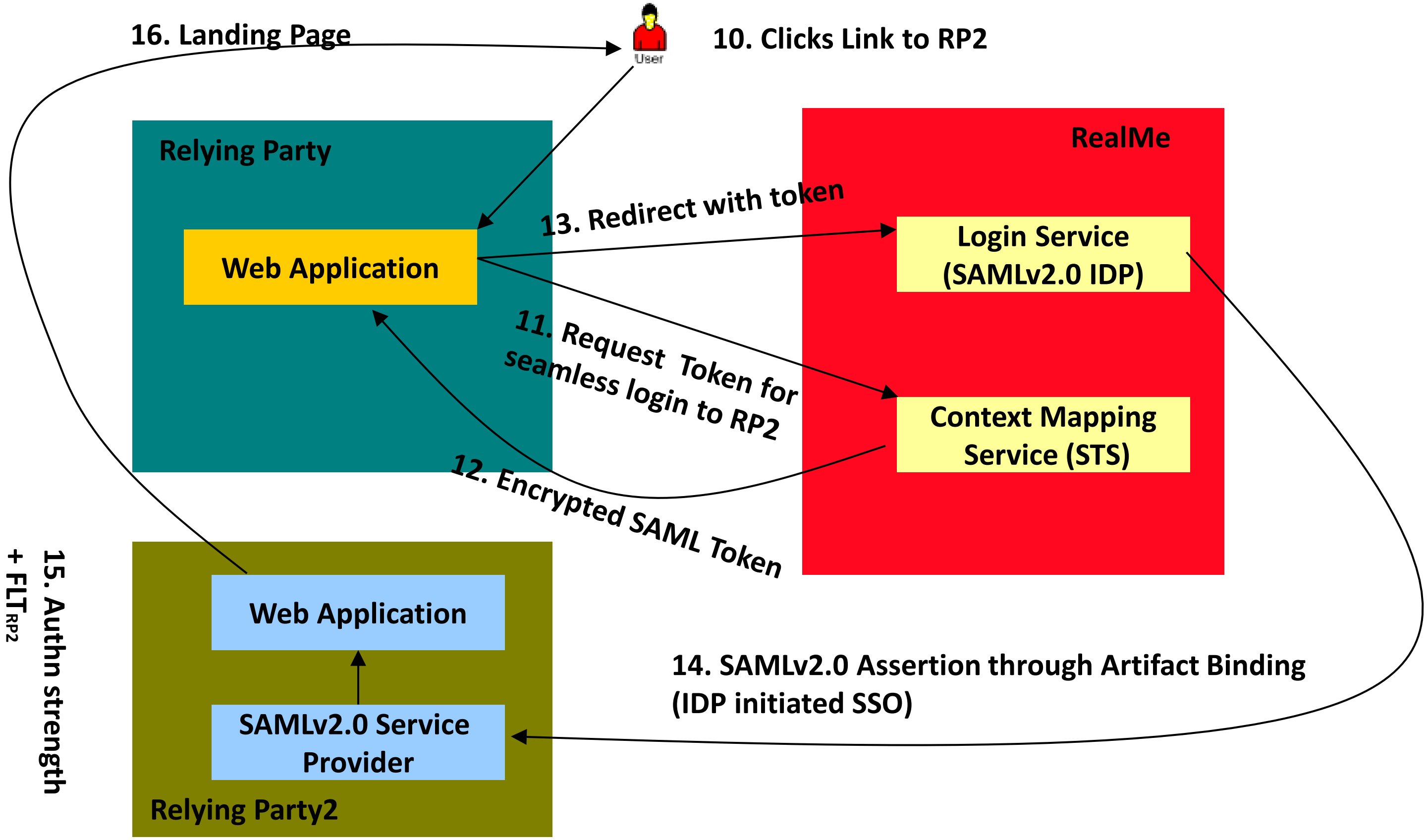
L3 – Seamless Login

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


16. Landing Page
User
10. Clicks Link to RP2
Relying Party
Web Application
RealMe
13. Redirect with token
Login Service (SAMLv2.0 IDP)
11. Request Token for seamless login to RP2
Context Mapping Service (STS)
12. Encrypted SAML Token
15. Authn strength + FLTRP2
Web Application
SAMLv2.0 Service Provider
Relying Party2
14. SAMLv2.0 Assertion through Artifact Binding (IDP initiated SSO)

Login Integration Patterns

L3 – Seamless Login

Technical Integration Specification

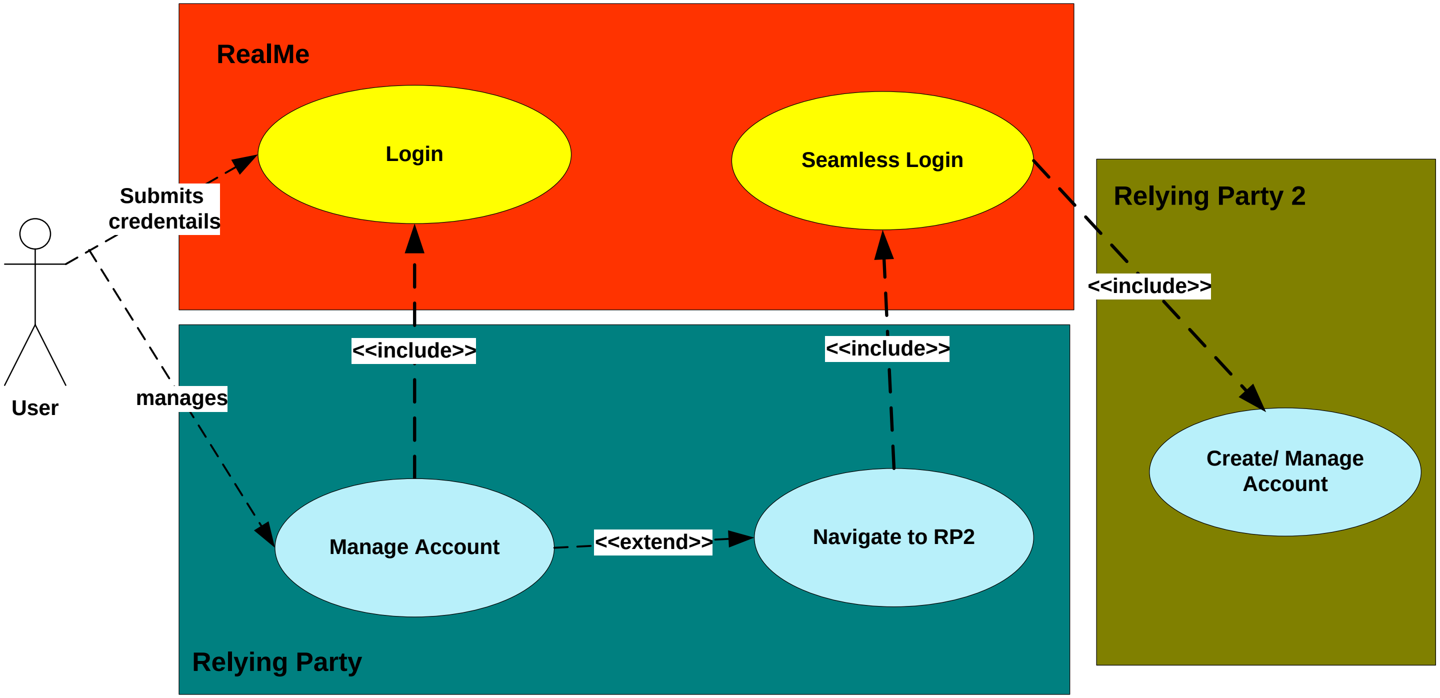
Integration Standard: SAMLv2.0, WS-Trust 1.4

- **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 Verified Account

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.**

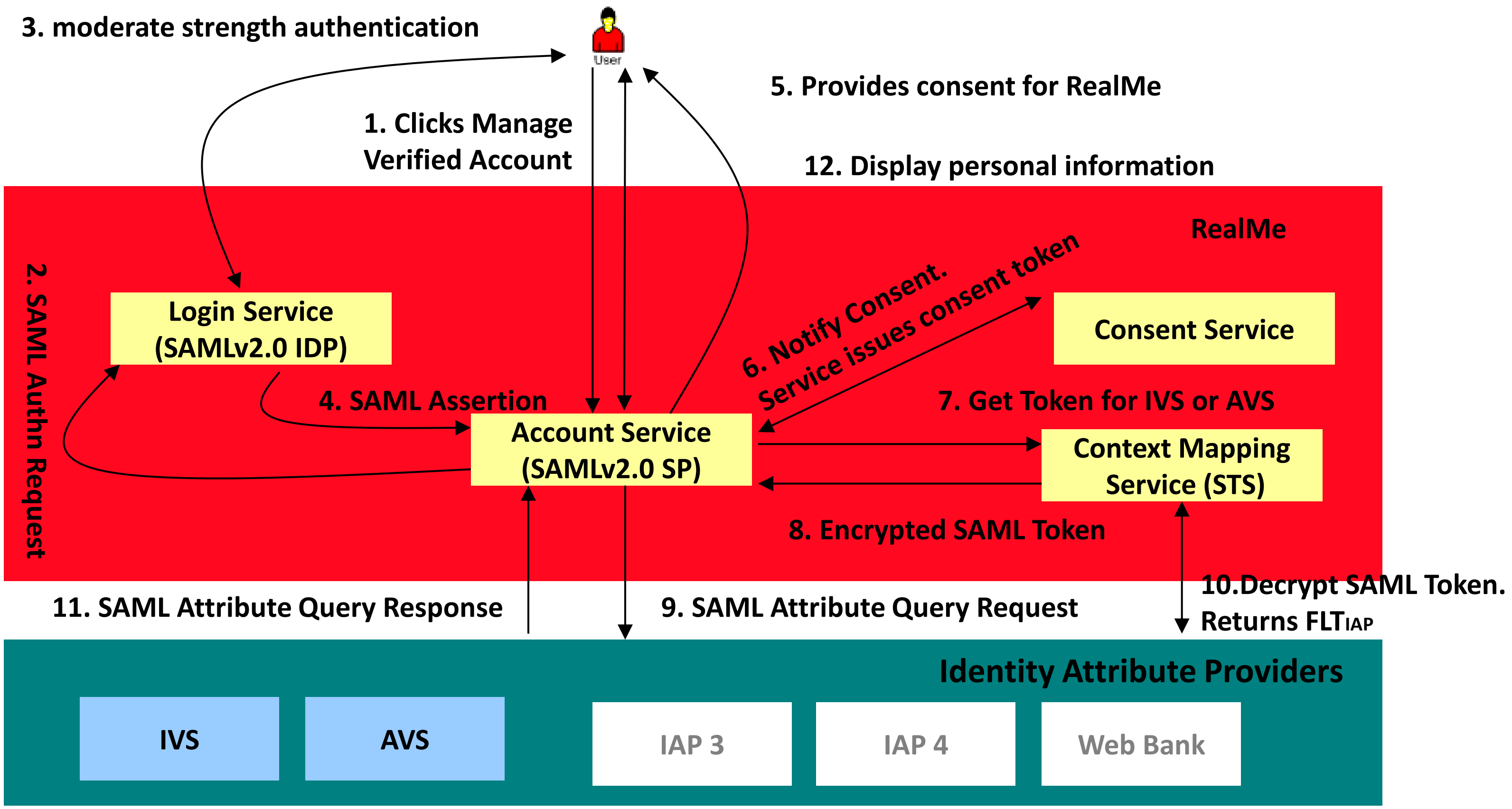
IAP Integration Patterns

- **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



3. moderate strength authentication
User
1. Clicks Manage Verified Account
5. Provides consent for RealMe
12. Display personal information
RealMe
2. SAML Authn Request
Login Service (SAMLv2.0 IDP)
6. Notify Consent. Service issues consent token
Consent Service
4. SAML Assertion
7. Get Token for IVS or AVS
Account Service (SAMLv2.0 SP)
Context Mapping Service (STS)
8. Encrypted SAML Token
10.Decrypt SAML Token. Returns FLTIAP
11. SAML Attribute Query Response
9. SAML Attribute Query Request
Identity Attribute Providers
IVS
AVS
IAP 3
IAP 4
Web Bank

IAP Integration Patterns

IAP1 – Get Status or Personal Information

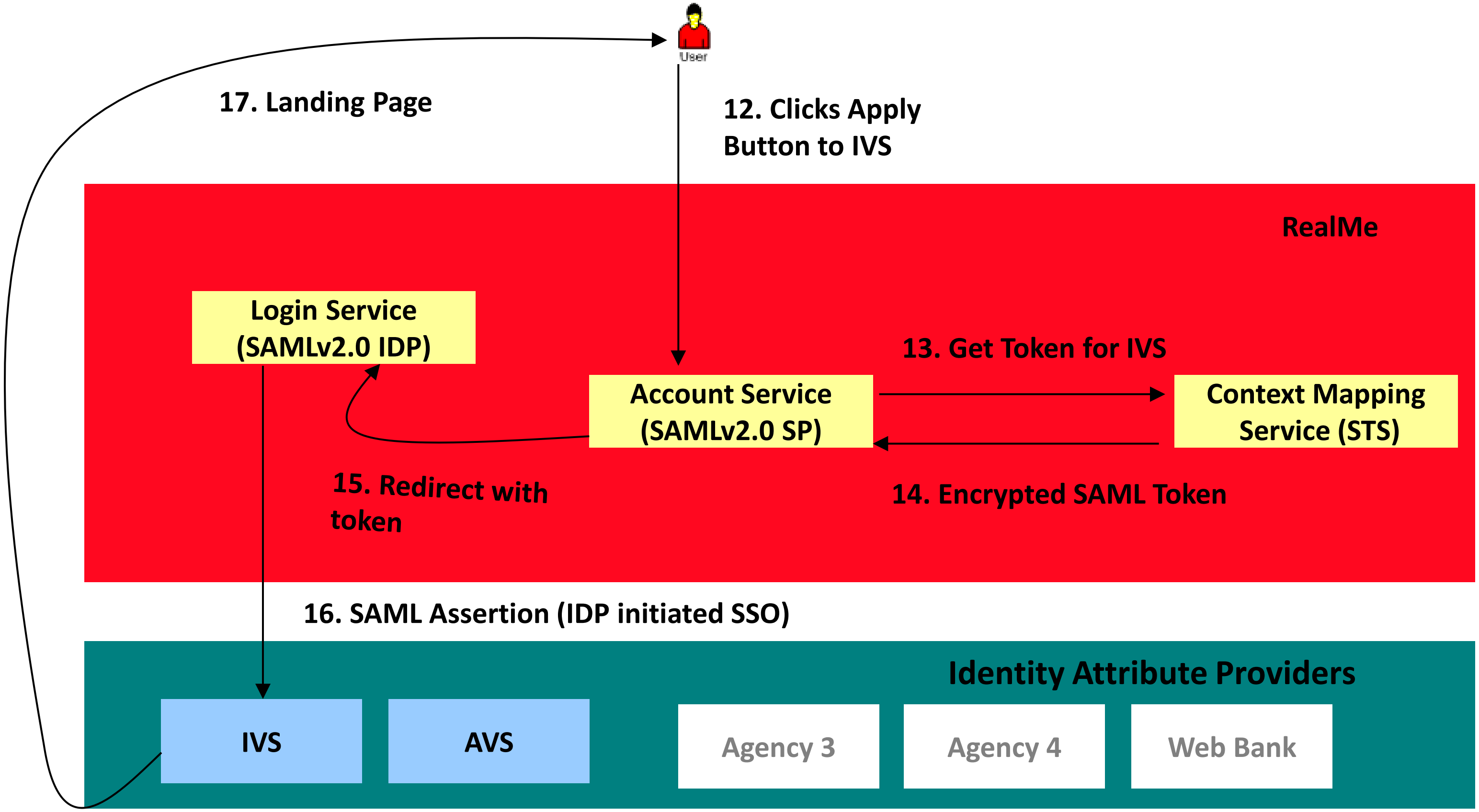
Technical Integration Specification

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



User
17. Landing Page
12. Clicks Apply Button to IVS
RealMe
Login Service (SAMLv2.0 IDP)
13. Get Token for IVS
Account Service (SAMLv2.0 SP)
Context Mapping Service (STS)
15. Redirect with token
14. Encrypted SAML Token
16. SAML Assertion (IDP initiated SSO)
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**

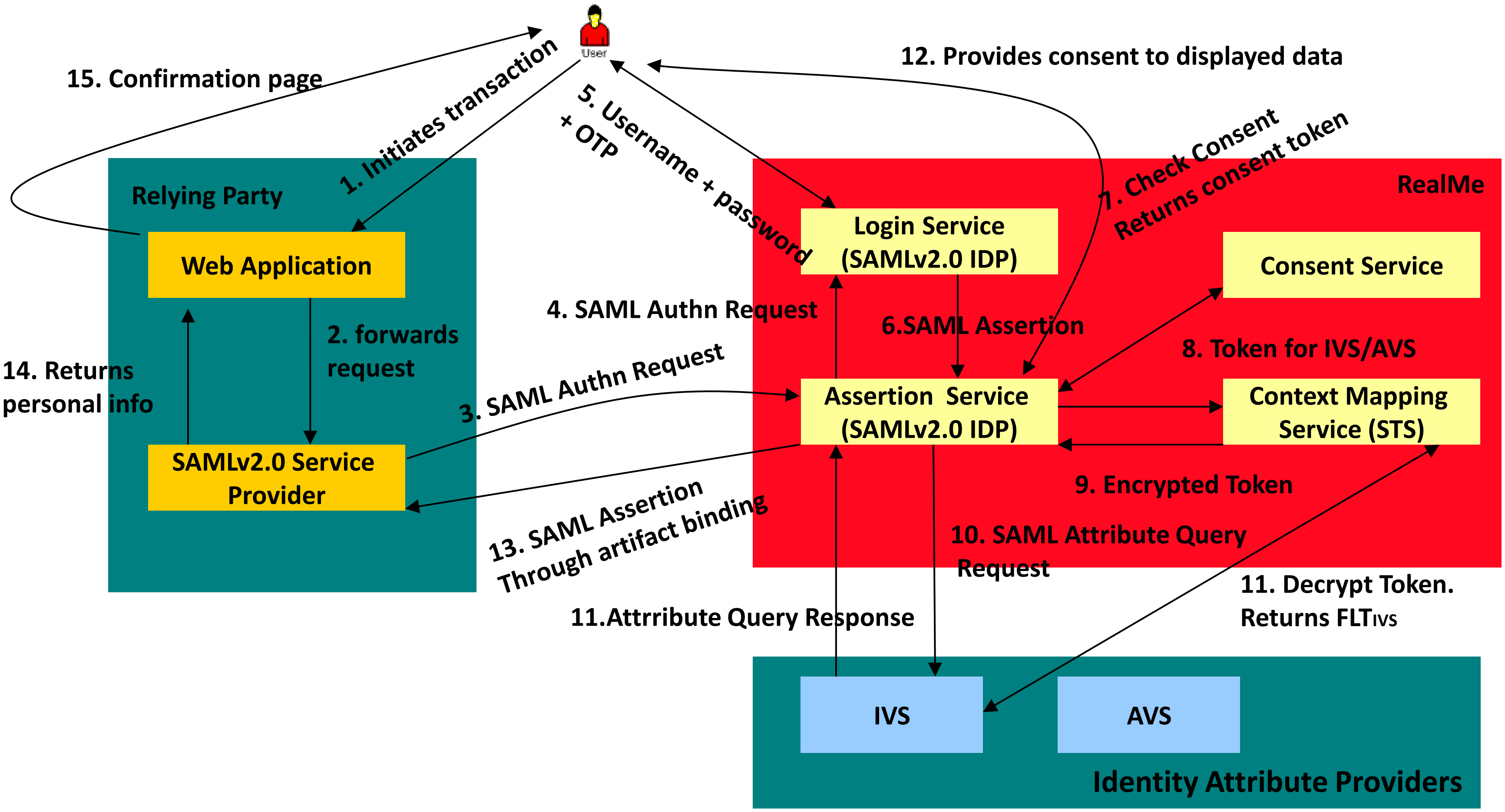
Identity Assurance integration patterns
A1 – Assert only

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


User
15. Confirmation page
1. Initiates transaction
5. Username + password + OTP
12. Provides consent to displayed data
Relying Party
Web Application
2. forwards request
14. Returns personal info
SAMLv2.0 Service Provider
3. SAML Authn Request
4. SAML Authn Request
13. SAML Assertion Through artifact binding
RealMe
Login Service (SAMLv2.0 IDP)
6.SAML Assertion
7. Check Consent Returns consent token
Consent Service
8. Token for IVS/AVS
Assertion Service (SAMLv2.0 IDP)
Context Mapping Service (STS)
9. Encrypted Token
10. SAML Attribute Query Request
11.Attrribute Query Response
11. Decrypt Token. Returns FLTIVS
IVS
AVS
Identity Attribute Providers

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.

RealMe

Questions ???