New Zealand Post

INTERNAL AFFAIRS
Te Tari Taiwhenua

RealMe

Technology Solution Overview

Version 1.0 – *Final*

September 2012

Authors: Mick Clarke & Steffen Sorensen

What is RealMe?

RealMe is a product that offers identity services for people to use and manage online. A user will have a RealMe Account that will provide the following functions:

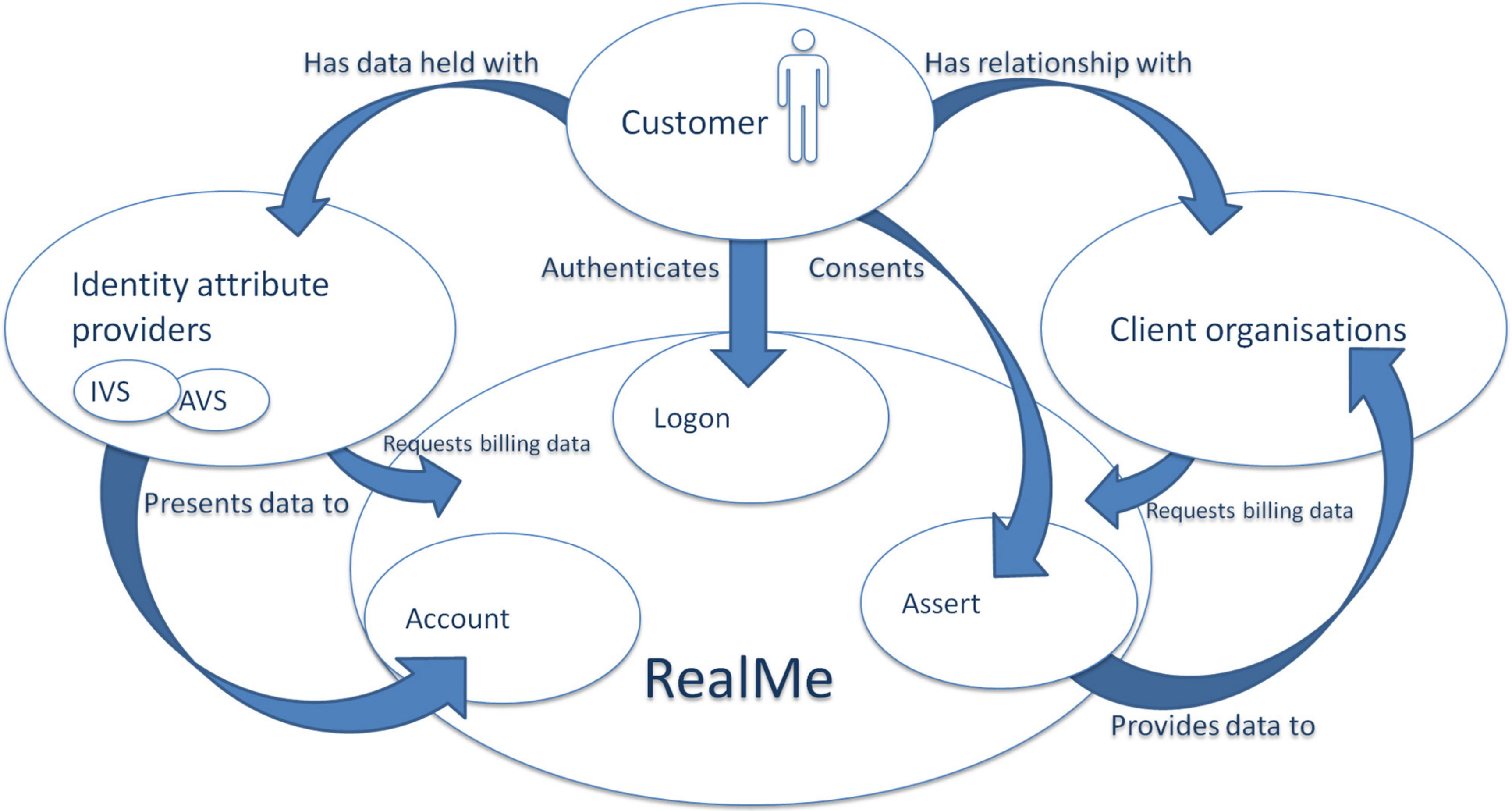
Authentication: Logon Service

- A single username and password to access online services. People will be able to "*sign-in*" or "*log in*" with RealMe at a wide range of websites;
- People can use RealMe to provide a second factor when accessing online services. This maybe a one-time SMS code or a secure token.

Online data provision: Assertion Service

- A means to collate information that various organisations hold about them and provide it securely online to other organisations;
- In particular they can provide the attributes held within the igovt identity verification service (IVS), namely, full name, date of birth, place of birth and gender, that assures their identity has been established to a high standard.

RealMe Context



RealMe Principles

Ease of Use

- Ensure that RealMe is easy to use.

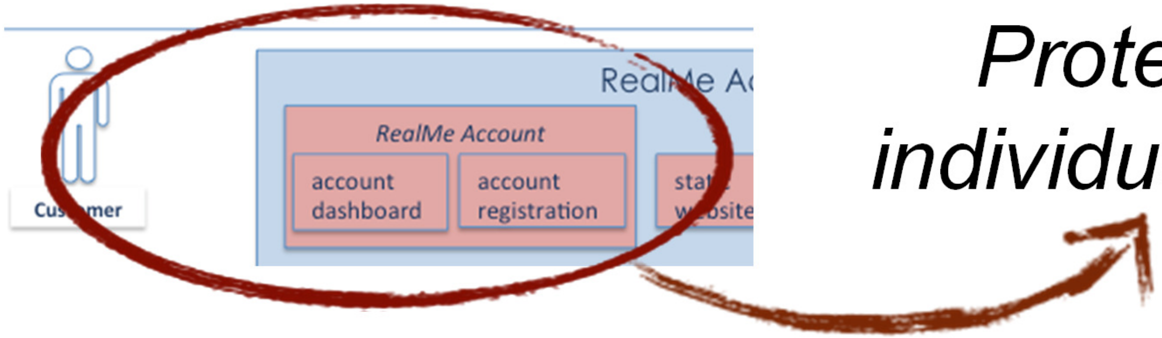
Privacy Protection

- Ensure that the solution protects an individual’s privacy by design.

Information Security

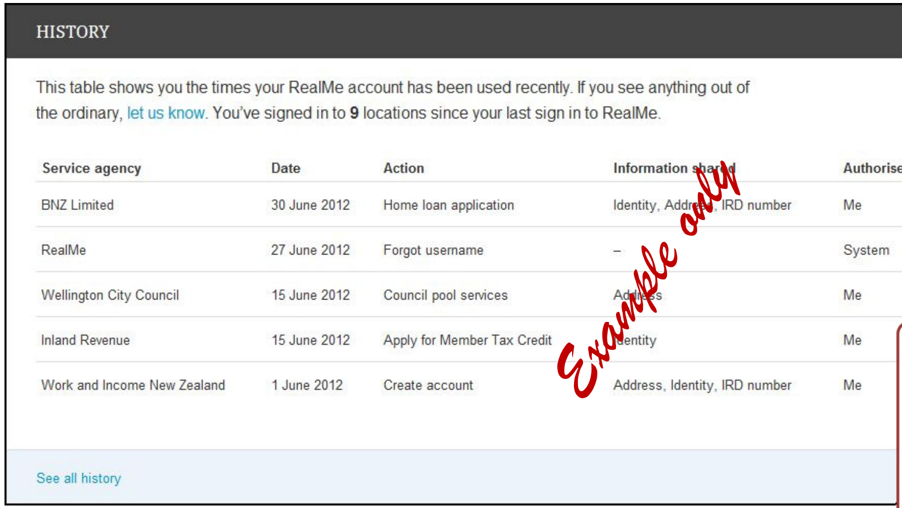
- Ensure that the solution is secure and any data is suitably protected to a high level.

RealMe Account



Protecting an individual's privacy

Usage Reports



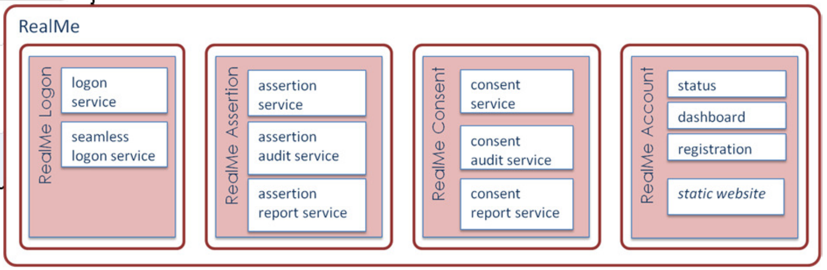
HISTORY

This table shows you the times your RealMe account has been used recently. If you see anything out of the ordinary, let us know. You've signed in to **9** locations since your last sign in to RealMe.

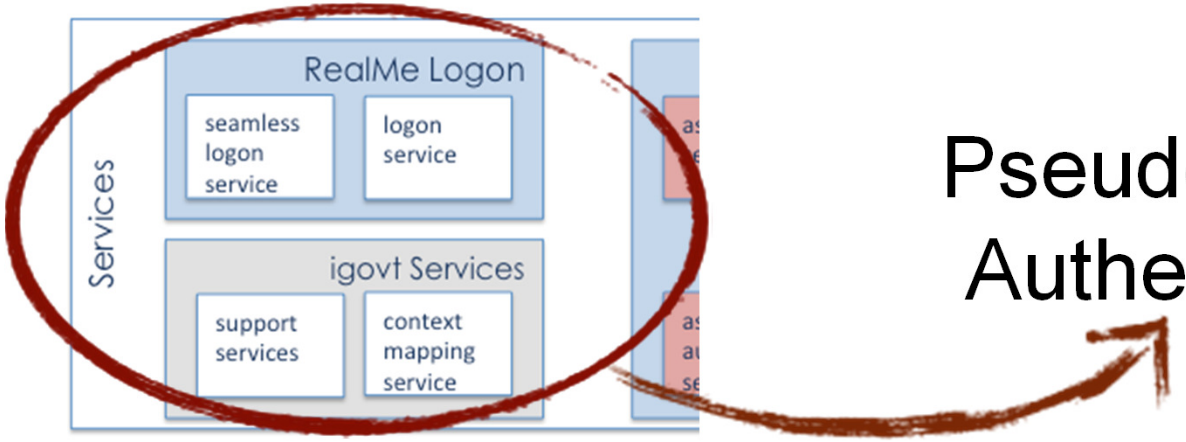
Service agency	Date	Action	Information shared	Authorised by
BNZ Limited	30 June 2012	Home loan application	Identity, Address, IRD number	Me
RealMe	27 June 2012	Forgot username	–	System
Wellington City Council	15 June 2012	Council pool services	Address	Me
Inland Revenue	15 June 2012	Apply for Member Tax Credit	Identity	Me
Work and Income New Zealand	1 June 2012	Create account	Address, Identity, IRD number	Me

See all history

Privacy Domains



RealMe Authentication - Logon

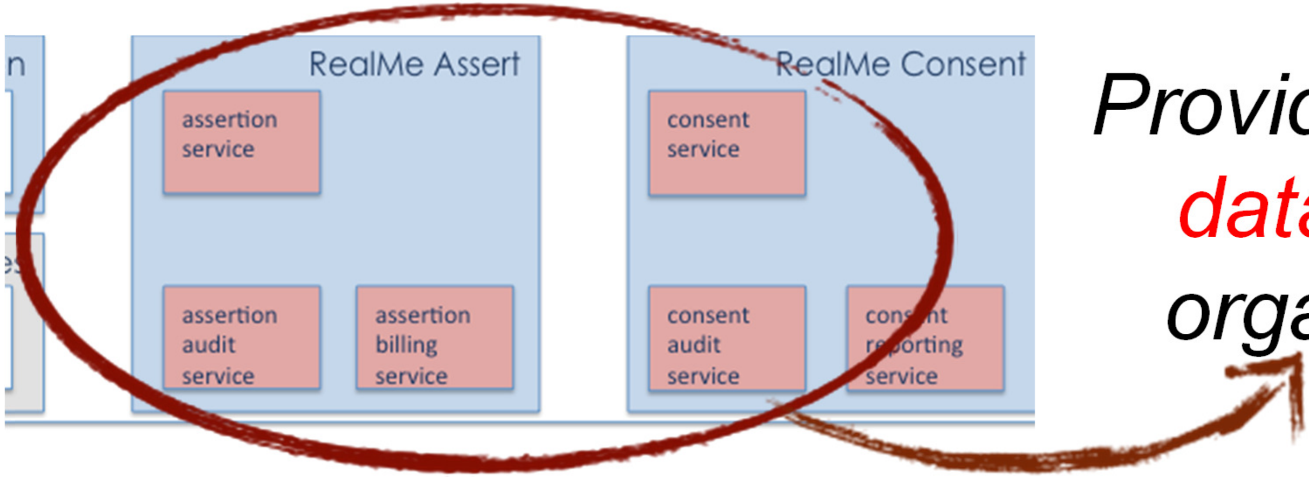


Pseudonymous Authentication

Provides

- Managed authentication service;
- No single identifier.

RealMe Verified Data - Assertion

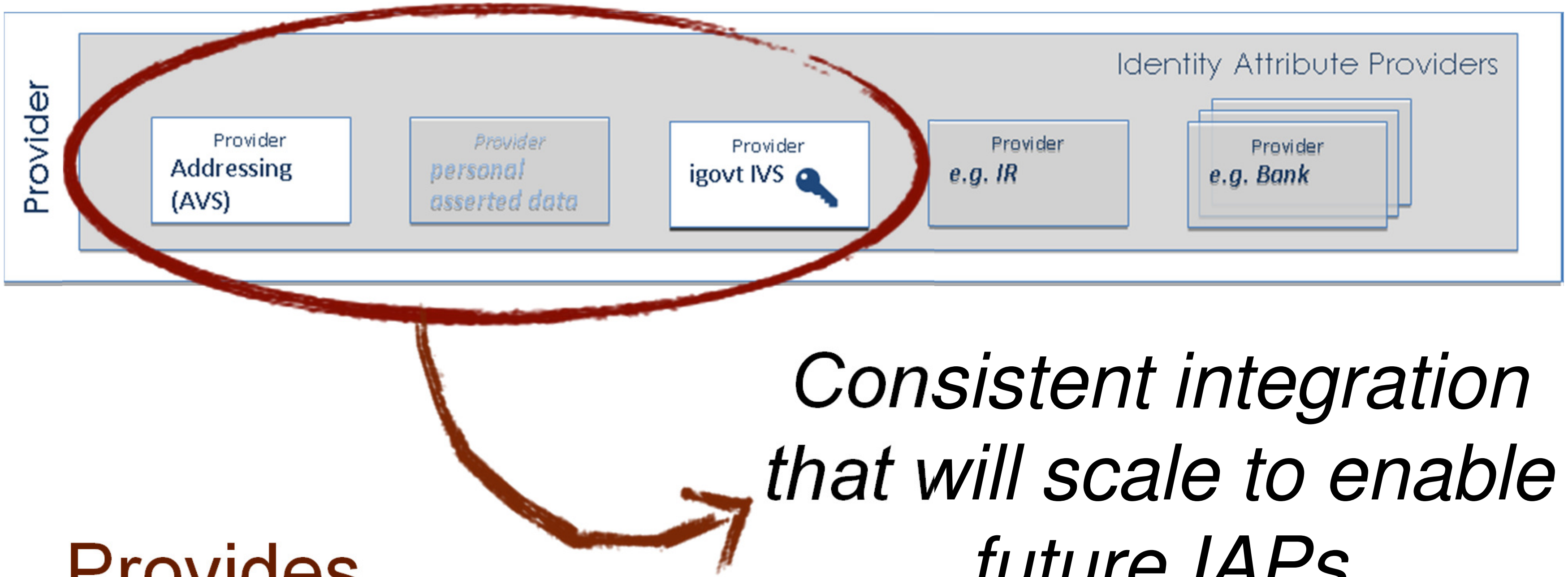


Providing verified data to client organisations

Provides

- A secure, privacy-centric data exchange;
- A clear consent model;
- An extensible data set across multiple providers.

RealMe Identity Attribute Providers



Consistent integration that will scale to enable future IAPs

Provides

- Access to data held with multiple providers;
- A means of aggregating data in real-time.

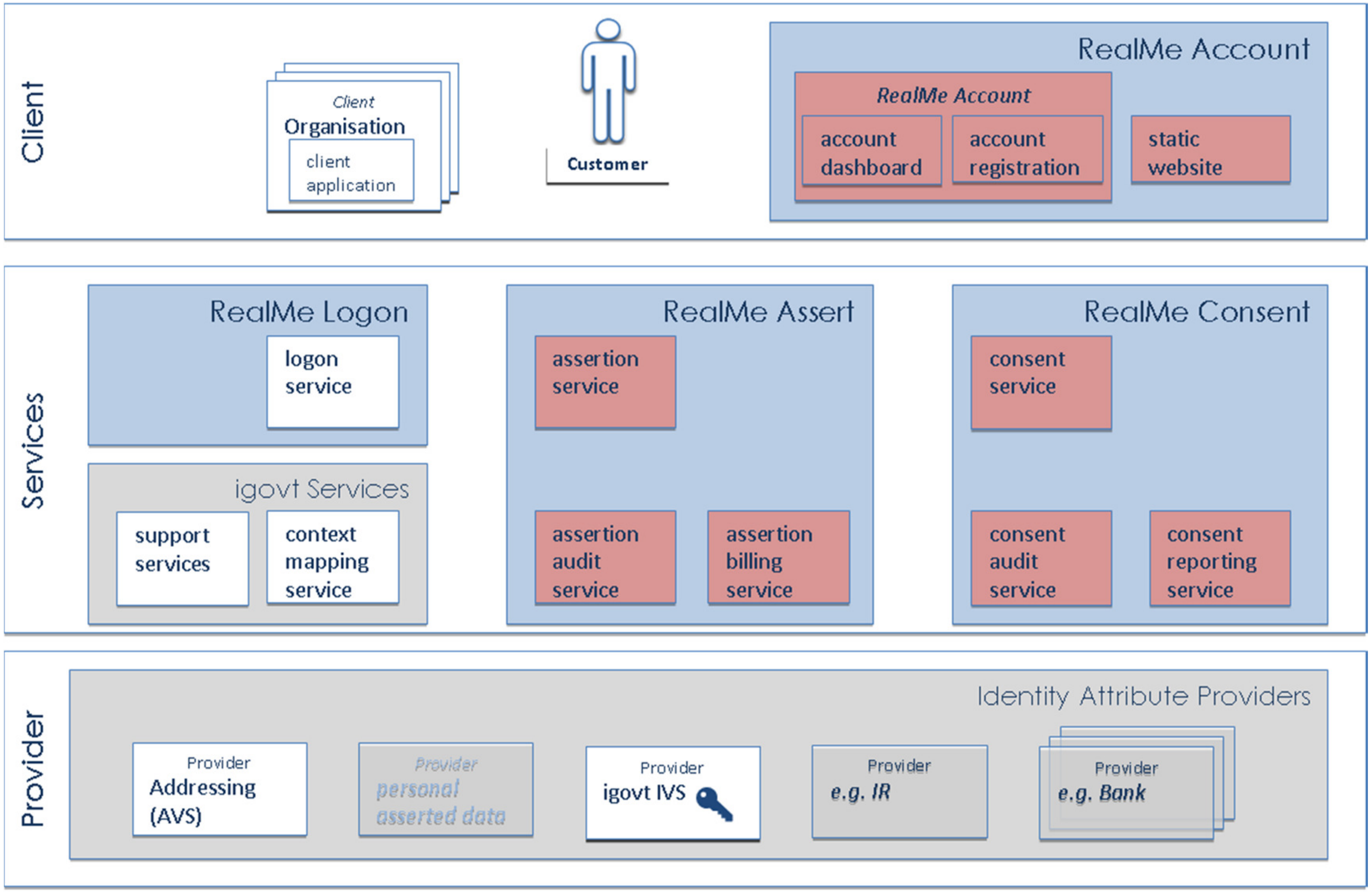
How is RealMe Used?

Service usage	Function	Example Usage	Status
Logon only	Enables a RealMe customer to authenticate at an integrated client site.	When a customer wants to use an online service securely, they can use their RealMe Account to do so using the same username and password they use at many other online services. In some cases the online service requires a greater level of security; RealMe can provide this by means of a "second factor" by means of a one time SMS code or via a secure token they possess.	Existing igovt solution (2012)
Extended Logon	Enables a RealMe customer to authenticate at one integrated client site and then navigate seamlessly to another participating client site without requiring re-authentication.	RealMe provides customers a username and password that can be used across a number of online services. In some cases if a customer is "signed-in" at one service they will not be required to enter their username and password to access another service. This works well for those services that are linked in a business sense, or are part of a suite of services within a single organisation.	Existing igovt solution (2012)
Assert only	Enables a RealMe customer to provide identity data at an integrated client site.	A customer wants to enrol for an online service or apply for, say, a home loan online; they need to provide information about themselves and provide proof of identity. They can do this using their RealMe Account. They would log into RealMe and consent to provide information about themselves for the service they require. The data is then securely sent, including data that proves who they are. This replaces the need for a customer to have to prove their identity face to face and allows them to complete the transaction wholly online.	New solution (2013)

How is RealMe Used?

Service usage	Function	Example Usage	Status
Assert then Logon	Enables a RealMe customer to provide identity data at an integrated client site and pass back a valid logon service token to allow future re-authentication for that online service.	A customer enrols or applies for an online service and provides information about themselves and proves their identity online. They can also provide their logon, or “sign-in” key to the service provider at this point. This enables the customer who has applied for a home loan, to later logon, or “sign-in”, with RealMe to view securely the status of their loan application.	New RealMe solution (2013)
Logon then Assert	*Enables a RealMe customer to authenticate at an integrated client site and then seamlessly provide identity data to that client within the same session.*	*A customer would have used their RealMe Account to logon to an online service, say, for example, Internet Banking. They may also need to use their RealMe Account to prove their identity to authorise a transaction (say, a high value payment). They would already be logged into with RealMe, but would require a second factor “step-up”, say an SMS code sent to their mobile phone in order to prove their identity. This scenario would be supported by RealMe.*	*Roadmap item - may require new SAML message profile.*
Federated Logon	*Enables a RealMe customer to authenticate at a client site using the client-centric credentials, then to seamlessly use their RealMe authentication credentials for second factor, or verification purposes.*	*Some organisations would like to retain their own authentication mechanisms, such as Internet Banking. RealMe intends to support this by enabling organisations joining RealMe as Identity Providers (IDPs). In this case, if a customer were to log onto their Internet Banking site, they would also be logged onto the RealMe domain, enabling access to the RealMe services as if logged in through RealMe directly.*	*Roadmap item*

RealMe Architecture Overview



Client

Client Organisation

client application

Customer

RealMe Account

RealMe Account

account dashboard

account registration

static website

Services

RealMe Logon

logon service

igovt Services

support services

context mapping service

RealMe Assert

assertion service

assertion audit service

assertion billing service

RealMe Consent

consent service

consent audit service

consent reporting service

Provider

Identity Attribute Providers

Provider Addressing (AVS)

Provider *personal asserted data*

Provider igovt IVS

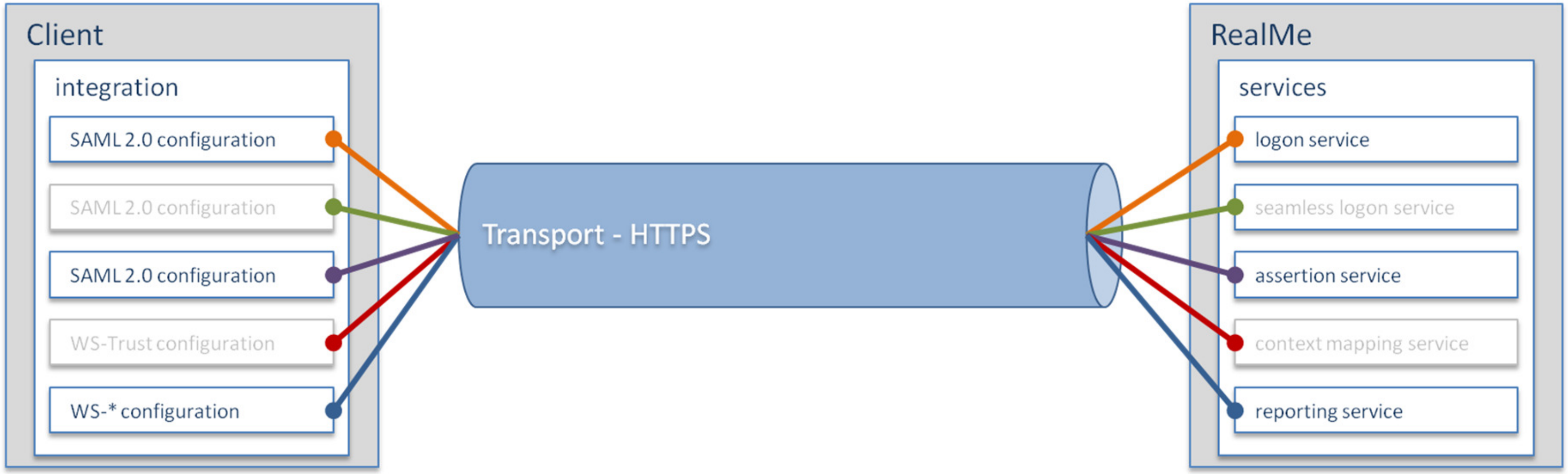
Provider *e.g. IR*

Provider *e.g. Bank*

Key	
	🟦 RealMe solution scope
	🟥 New components for RealMe
	Key RealMe identity data 🔑

newzealand.govt.nz New Zealand Post

Integrating to RealMe



Common means of integration

- *Clients choose the RealMe services they require;*
- *Integration configurations are provided supporting each service.*

RealMe Standards

Aligned with Government Enterprise Architecture of NZ (GEA-NZ)

Standards-based, compliant solution:

- GEANZ (e-GIF) standards
- NZ SAMS (an OASIS SAML 2.0 Profile)
  - SP initiated SSO flow.
- NZ Secure Web Services Standards (a WS-I Basic/OASIS WS-Trust/WS-Security/SOAP Profile)
  - Issue and Validate binding.
- NZ CIQ (an OASIS CIQ v3 Profile)
  - Identity information message format
- Authentication Key Strengths (and the subset Password) Standard (amendments)
- New Zealand Government Web Standards V2.0;
- New Zealand Security Manual (NZISM)
  - general security and specifically cryptography
- Security in the Government Sector (SIGS)

Non-Functional Requirements

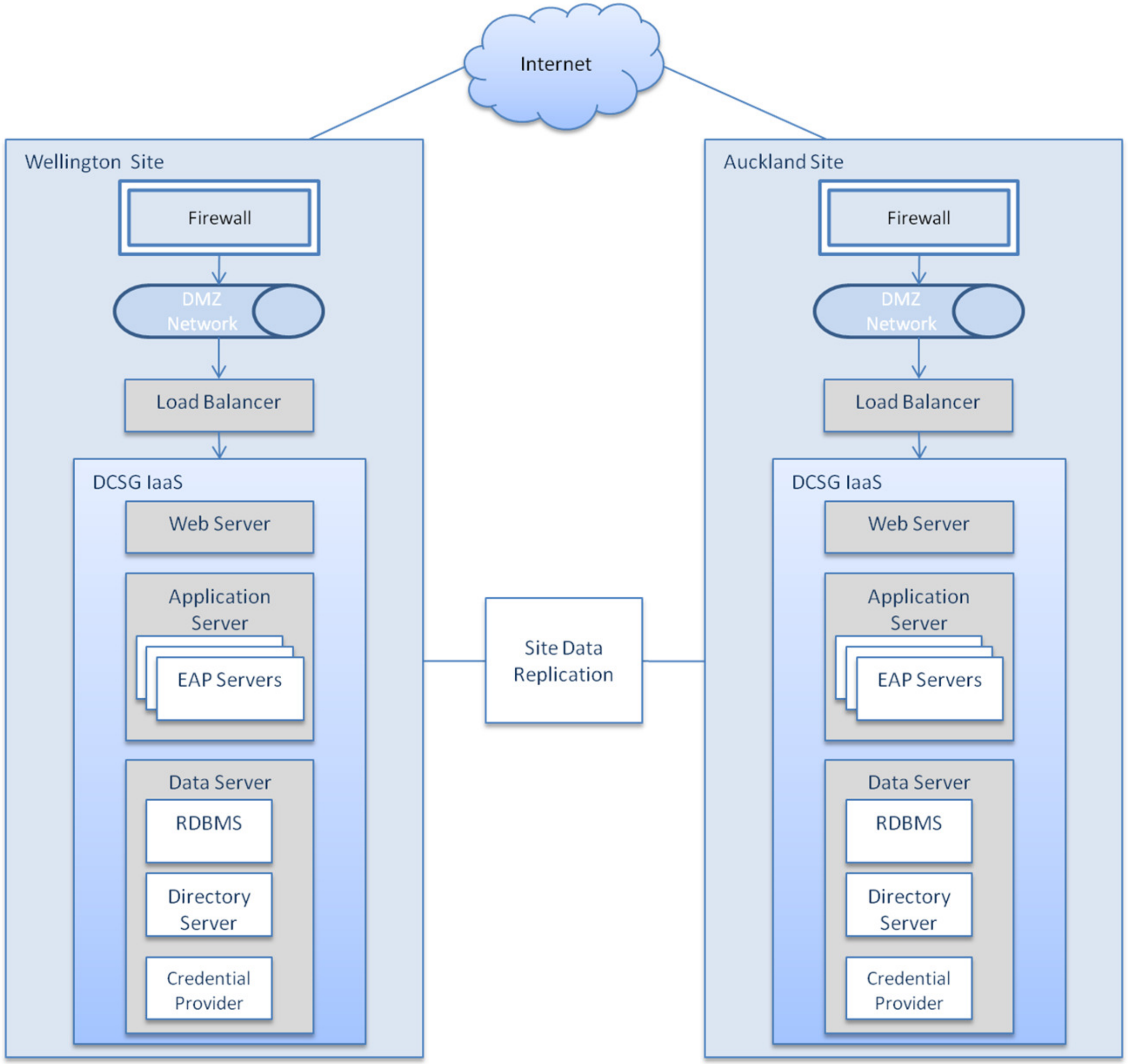
Top Level – for Day One 2013

- *Availability – 99.95% (including planned outages);*
- *Performance – sub-second response times;*
- *Capacity – 30 requests per second.*

Solution Platform

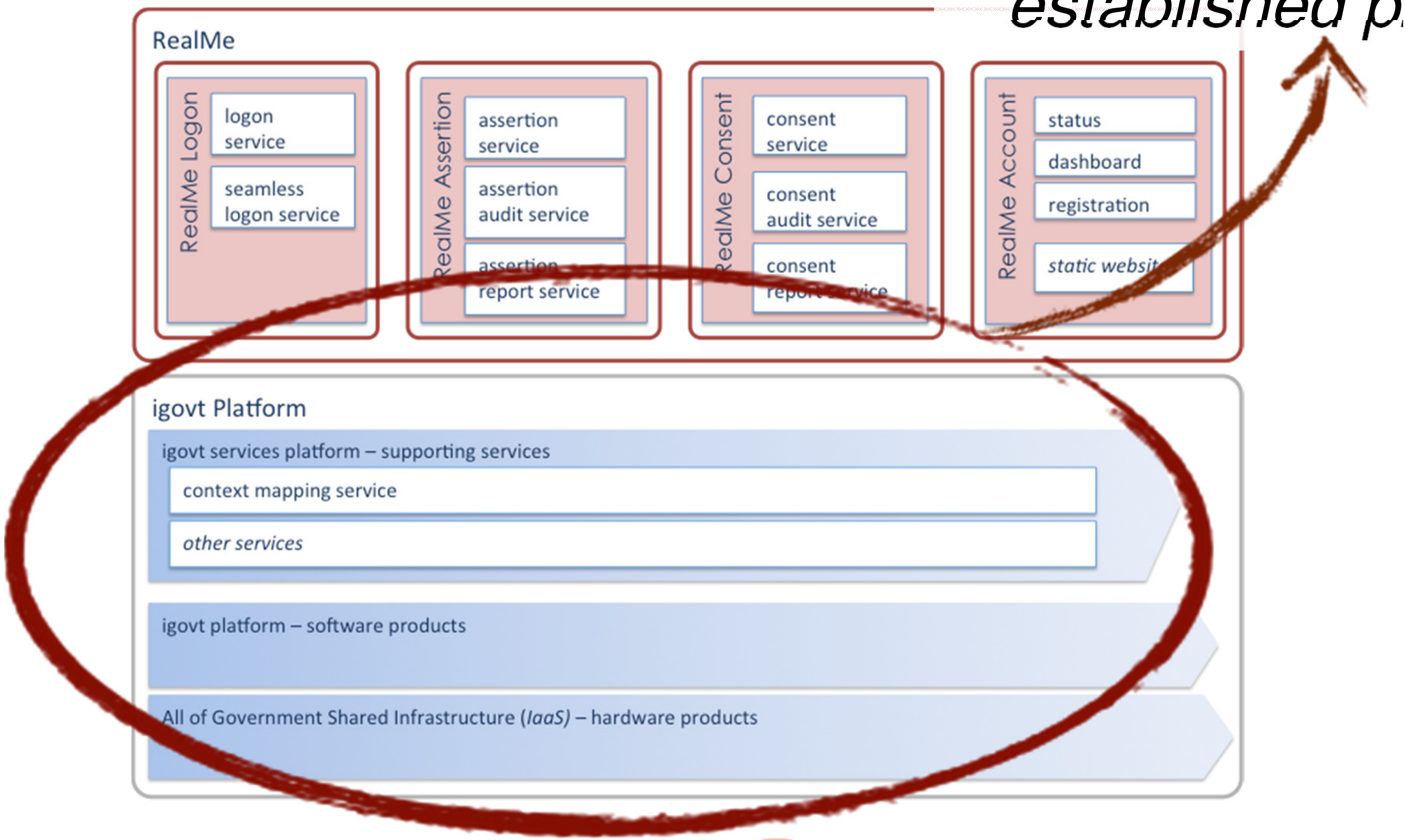
- *Dual site, geographically separated;*
- *Active-active, fully redundant configuration;*
- *Scalable infrastructure to meet future demand.*

RealMe Solution Hosting



RealMe Solution Platform

Re-use and extension of established platform



RealMe

RealMe Logon
- logon service
- seamless logon service

RealMe Assertion
- assertion service
- assertion audit service
- assertion report service

RealMe Consent
- consent service
- consent audit service
- consent report service

RealMe Account
- status
- dashboard
- registration
- *static websit*

igovt Platform

igovt services platform – supporting services
- context mapping service
- *other services*

igovt platform – software products

All of Government Shared Infrastructure (*IaaS*) – hardware products

RealMe - Roadmap

Add the missing services

- *Logon then Assert flow (new SAML profile);*
- *Fully Federated Logon – support for third-party IDPs.*

Additional IAPs

- *government-held identity attributes, such as IRD number or drivers license details;*
- *Banks.*

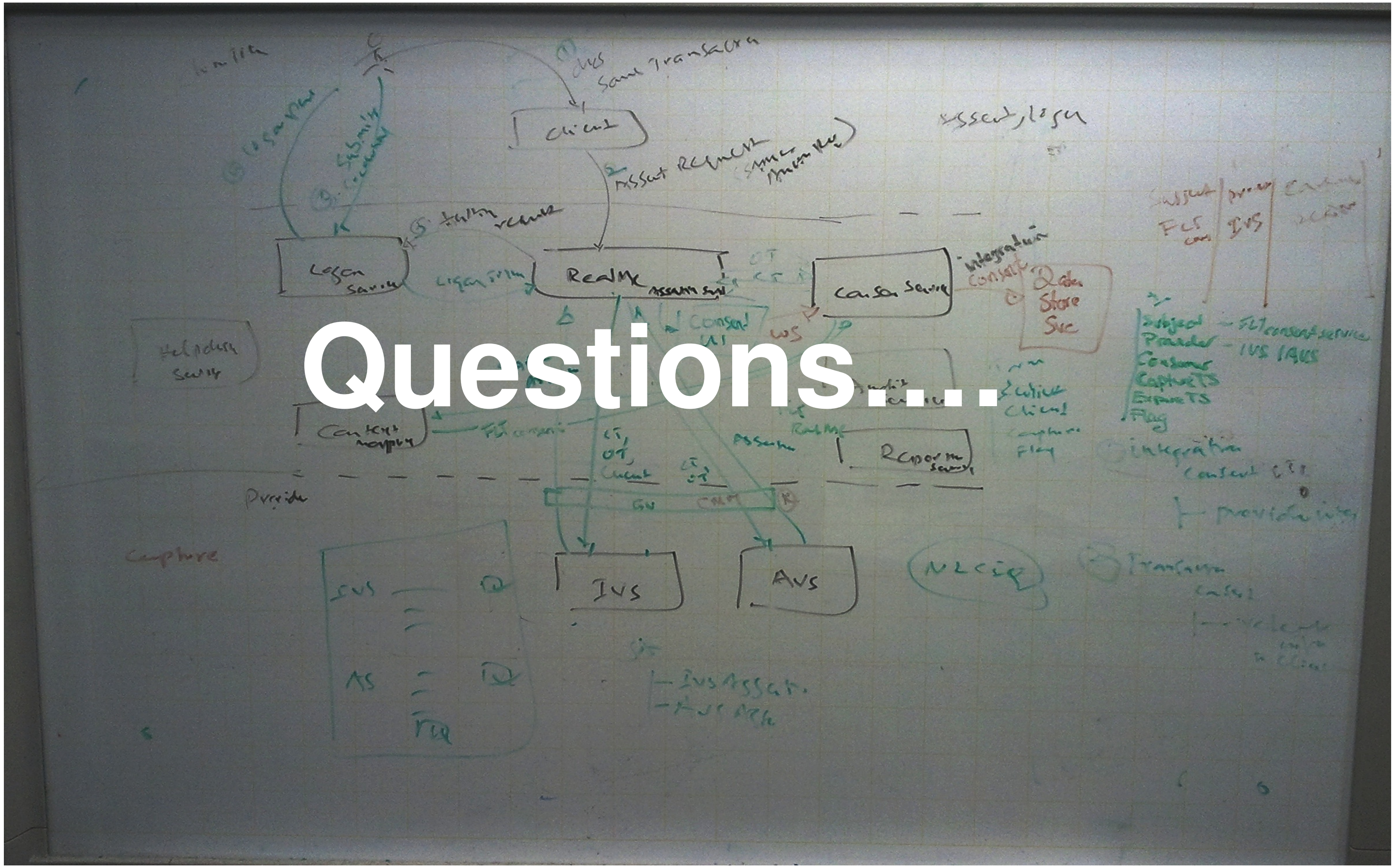
Online banking

- *Transaction authorisation;*
- *Verification.*

Technical Capabilities

- *Additional mechanisms for multi-factor authentication;*
- *Full mobile support;*
- *Voice biometrics support.*

RealMe - Detailed Solution



Questions.....