New Zealand Report Card: ‘Still in the leading bunch – more to do’

Personal analysis & observations

Government (Internal Affairs Dept)

NZ Post (an SOE)

http://realme.govt.nz
Background: New Zealand’s culture, policy and legislation

- Privacy legislation (EU-like) e.g. citizen controls use of/ release of data
- No national ID or ID card, no exchange of biometrics
- Low national security or illegal immigration drivers
- No Inter-agency data matching excl. few exceptions
- Citizen opt-in: Not compelled to use online services
- Agency opt-in: Not compelled to deliver via online
- Low risk, low budget approach (population: 4m)
Policy principles that are reflected elsewhere...

<table>
<thead>
<tr>
<th>NZ Govt policy principles (2002) for authenticating people</th>
<th>US NSTIC’s guiding principles (2011)</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Security</td>
<td>– Secure &amp; Resilient</td>
</tr>
<tr>
<td>– Acceptability</td>
<td>– Easy to use</td>
</tr>
<tr>
<td>– Protection of privacy</td>
<td>– Privacy enhancing</td>
</tr>
<tr>
<td>– All-of-government approach</td>
<td>– Interoperable</td>
</tr>
<tr>
<td>– Fit for purpose</td>
<td>– Cost effective</td>
</tr>
<tr>
<td>– Opt-in</td>
<td>– Voluntary</td>
</tr>
</tbody>
</table>
Back in 2005 we set out to address 3 issues
The First Issue
The Second Issue

• Keeping track of username and password for each online service was bad enough.

• We knew it would become worse when online services moved to two-factor authentication: “Necklace of tokens.”
And The Third Issue

- People have to use documents to establish their identity with each government agency individually.
Our approach to online authentication

- Two foundation services – both centralised but separate – identity and logon management
- Separate who a person is (identity) - from logon management functions - from what they do (activity)
- Decentralise authorisation and privilege management out to the edge

Name = Joe Bloggs
Date of birth = 01/01/1970
Place of birth = Wellington
Sex = male

Username = joe, Password = vT%5jnL
So we built 2 separate things:

- igovt pseudonymous logon service

- igovt Identity (attribute) Verification Service (IVS) that releases identity info or pseudo hashes has explicitly directed by the identity owner
Architecture for logon Authentication – 2006/7

- pseudonymous logon management (the FLT) carries no PI, designed in privacy and security with functions separated
- Take off the bottom row and the last column: what do you see?

<table>
<thead>
<tr>
<th></th>
<th>Credential</th>
<th>Credential Serial Number</th>
<th>Federated Logon Tag</th>
<th>Personal Identity information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential/Key</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provider</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Government Logon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Agency</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service User</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CROWN COPYRIGHT ©
‘OMB M 04 04 – like’ Identity proofing – maybe extendable to organisations, software, devices - online

<table>
<thead>
<tr>
<th>EOI objective</th>
<th>Low EOI Confidence Level</th>
<th>Moderate EOI Confidence Level</th>
<th>High EOI Confidence Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A – Identity exists</strong> (i.e. to determine that the identity is not fictitious)</td>
<td>1 document</td>
<td>1-2 documents (including at least one with photograph, if possible)</td>
<td>1-2 documents (including at least one with photograph, if possible) or Verification against 1-2 source records held by issuing agency</td>
</tr>
<tr>
<td><strong>B – Identity is a ‘living identity’</strong></td>
<td>(No specific process)</td>
<td>(No specific process)</td>
<td>Verification against the death register or Business processes for Objective C</td>
</tr>
<tr>
<td><strong>C – Presenter ‘links’ to identity</strong></td>
<td>(No specific process)</td>
<td>Verification by trusted referee or In-person verification</td>
<td>Verification by trusted referee or In-person verification or Biometric recognition where the agency has authorised access to a database containing the individual’s biometric information and Interview (in cases where suspicion is raised over individual’s identity)</td>
</tr>
<tr>
<td><strong>D – Presenter is sole claimant of identity</strong></td>
<td>Check against agency records</td>
<td>Check against agency records</td>
<td>Check against agency records</td>
</tr>
<tr>
<td><strong>E – Presenter uses identity</strong> (i.e. use in the community)</td>
<td>At least 1 document/record</td>
<td>At least 1 document/record or Business processes for Objective C</td>
<td>At least 2 document/records or Business processes for Objective C</td>
</tr>
</tbody>
</table>
..and mapped to NZ’s ‘NIST 800-63-like’ Authn Credential Strength Standard .. looks dated now..

<table>
<thead>
<tr>
<th>Determine Service Risk Category</th>
<th>Apply applicable EOI Confidence levels</th>
<th>Apply applicable Authentication keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nil or negligible</td>
<td>None</td>
<td>No specific recommendation.</td>
</tr>
</tbody>
</table>
| Low | - EOI genuine and identity used in community.  
- EOI accepted on ‘face value’. | One-factor key:  
-Password conforming to the *Password Standard* e.g. igovt password. |
| Moderate | - EOI genuine and identity used in community.  
- Individual confirmed as genuine claimant of the identity.  
- EOI accepted on ‘face value’. | Two-factor key that is at least:  
- One-time password system + password e.g. igovt password and igovt code.  
- One-time password device + per-session activation with a password or a biometric.  
- Software token + per-session activation with a password or a biometric. |
| High | - EOI genuine and identity used in community.  
- Individual confirmed as genuine claimant of the identity.  
- EOI verified by third party. | Two-factor key that is at least:  
- Hardware token + per-session activation with a password or biometric. |
In 2010/11 the government wanted a partner to leverage what it had built...

enter ..

about the time the US NSTIC was being drafted
Confirms that this is the same dog/person/entity as last interaction

Consistency

Confirms core identity information from Internal Affairs’ igovt identity Verification Service and address from NZ Posts Address Verification service

Uniqueness

Other providers to come

SP/RP has confidence in user’s identity (in advance of applying authz policy)
Confirms that this is the same dog/person/entity as last interaction.

Consistency

(login Service (currently igovt logon)) + (when needed) identity assurance services

Confirms core identity information from Internal Affairs’ igovt identity Verification Service and address from NZ Posts Address Verification service

Uniqueness

SP/RP has confidence in user’s identity (in advance of applying authz policy)

Other providers to come

Igovt  IVS

New Zealand Post  AVS
The + design introduces a portal and new loosely coupled services to accelerate federation with new partners, adoption of cloud services and emergence of personal cloud. The service suite, which is user accessible via SAML browser based front channel becomes: logon, assertion, consent, and the user’s account dashboard.
..it’s built but will they come?..

<table>
<thead>
<tr>
<th>Statistics pre- RealMe launch</th>
<th>(July 2013)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total logons</td>
<td>6M</td>
</tr>
<tr>
<td>Total logon citizen ‘accounts’</td>
<td>1.5m (30% of population)</td>
</tr>
<tr>
<td>Total igovtIDs created</td>
<td>0.37m</td>
</tr>
<tr>
<td>Govt agencies connected</td>
<td>14/43 services (40% central agencies) doing 14.8m transactions to date</td>
</tr>
</tbody>
</table>
‘Still in the leading bunch – more to do’
..personal observations.. Do you agree?

..the good

- NZ Post
- Supporting legislation
- Future-proofed privacy & SOA architecture patterns
- PR ‘wins’, such as online passport renewal
- Some signs of private sector engagement
- We’re up and going!

..improvement areas

- NZ Post
- Macro-economic/digital economy policy ‘lumpy’
- Governance with expert support
- ‘iGovt Logon only’ policy drives password resets
- Newer lighter protocols - OAuth, OpenID, JSON
- Mobile Authn/optimisation
- Organisation and device identity
- User centric/personal data notions
- Most of all – culture, mindset and attitude