Stronger Authentication in a Federated World

Bill Young
Government Technology Services
NZ State Services Commission
Quick Background of NZ Authentication

- “Commercial” IdP for any government Agency
- Policy Driven
  - Privacy
  - Security
  - Standards
- Evolutionary Development - Web Applications First
Our Big Drivers

- Privacy
- May not Disenfranchise any part of the Public
- Breadth of Scale in govt Departments
NZ AuthN & IdM Services

People

Internet

Govt Agencies

igovt

Logon Service

Future Authentication Services

Name
Date of birth
Place of birth
Sex

GLS
IVS

Verified
What’s our Challenge?

- Continuous Improvement of Services
- Risk-Based Approach to Security
  - Adapt to Evolving Threats
  - Match Pace with the New Services Provided to End Users
- Limit Barriers to Uptake
Typical Responses to the Need for Stronger Authentication

- Conventional
  - ‘Better’ Passwords
  - OTP Tokens
- Less Conventional
  - PKI
  - Biometrics
Passwords

“We need Stronger Passwords. Let’s improve our Password Policy”

- Longer more complex passwords, system generated passwords, password history, force frequent changes, etc.

And the Result?

- Un-usable, Un-Fit, Un-Friendly, Un-Supportable
- Support Costs
- Social Engineering

There are Ways to Improve Passwords (just rarely used)
One Time Passwords (OTP)

- Tokens
  - $$ - Token Cost & Logistics
- Bingo cards & TAN sheets
  - More Cost-Effective, but Frequently Copied
- Soft Tokens
  - Security & Usability Issues
- SMS
  - Good, Except for High Volume Use
PKI

- Soft Certificates
  - Issues with Usability and Security
  - Support Cost
- Centrally Stored
  - Ok, But not Really 2FA
- Smartcards, USB tokens
  - Hardware & OS Support is Incomplete
  - High Support Cost
Biometrics

More Questions than Answers…
That’s all fine, but...

...how does it contribute to a Risk-Based approach?
Context Sensitive Authentication

Definition:

“Authentication based on Real Time Risk Analysis”
Context Sensitive Approach

User Enters Application

UID/Password or Higher

Federated Identifier & Risk ‘Advice’

Device Detection

Requested AuthN Context

High Value/risk

5%

“Strong” AuthN

Requested AuthN Context

Increased value/risk

25%

OTP AuthN

Application/Resources

Real-time Risk Assessment

Low value/risk

70%

No Action Required

Continue With Application
OOB Authentication

Definition:

Out of Band Authentication requires that separate information channels are used for authentication and access.
Out of Band Authentication

User Enters Application

UID/Password or Higher

Perceived Channel Risk

Federated Identifier & Risk ‘Advice’

AuthnContext

Application/ Resources

AuthnContext

SMS

Email

Phone

OOB AuthN

Application Continues

NZ State Services Commission
Crown Copyright
Transaction Authentication/Verification

Definitions:

“Transaction Authentication Verifies that the Correct User is Requesting a Transaction”

“Transaction Verification Verifies that the Correct Transaction is Performed for the User”

I’m combining both under the term “Transaction Authentication”
Transaction Authentication

User Enters

UID/Password or Higher

Federated Identifier & Risk ‘Advice’

Application/ Resources

Perceived Transaction Risk

Transaction Context/Details

Application Continues

“You are about Transfer $2384.89 to Account #BNZ927846738. Enter OTP to Continue”
Putting it all Together

User Enters

UID/Password or Higher

Device Detection

5% High risk

Transaction Context

Transaction AuthN

AuthN Context

OOB AuthN

Application/Resources

Federated Identifier & Risk ‘Advice’

Real-time Risk Assessment

5% Perceived threat

20% Increased value/risk

70% Low value/risk

AuthN Context

Step Up AuthN

Continue With Application

No Action Required

NZ State Services Commission
Crown Copyright
Question?

Should Transaction AuthN be done using SAML Web SSO?

It’s an AuthZ problem too…
SAML Considerations

How do these techniques look from a SAML point of view?
# Context Sensitive Authentication

## Step Up Authentication

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML Spec</td>
<td>Well Supported</td>
</tr>
<tr>
<td>Liberty Interop</td>
<td>Not Specified – Optional in US eAuth profile</td>
</tr>
<tr>
<td>eGov Profile</td>
<td>Supported</td>
</tr>
<tr>
<td>Vendor Support</td>
<td>Becoming Well Supported</td>
</tr>
</tbody>
</table>
## Context Sensitive Authentication

Returning Risk Context to SP

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML Spec</td>
<td>Well Supported</td>
</tr>
<tr>
<td>Liberty Interop</td>
<td>Not Specified</td>
</tr>
<tr>
<td>eGov Profile</td>
<td>Not Specified</td>
</tr>
<tr>
<td>Vendor Support</td>
<td>Mixed</td>
</tr>
</tbody>
</table>
# OOB Authentication

Passing `<Subject>` to IdP

<table>
<thead>
<tr>
<th>SAML Spec</th>
<th>Well Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Liberty Interop</td>
<td>Not Specified</td>
</tr>
<tr>
<td>eGov Profile</td>
<td>Not Specified or Restricted</td>
</tr>
<tr>
<td>Vendor Support</td>
<td>Unknown, but doubtful</td>
</tr>
</tbody>
</table>
Transaction Authentication

Transaction Details and Context

<table>
<thead>
<tr>
<th>SAML Spec</th>
<th>Unanticipated – Some options available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Liberty Interop</td>
<td>Not Specified</td>
</tr>
<tr>
<td>eGov Profile</td>
<td>Not Specified</td>
</tr>
<tr>
<td>Vendor Support</td>
<td>Unknown, but doubtful</td>
</tr>
</tbody>
</table>
Moving Forward

- Look at Real Time Risk Analysis
  - Need an easy model for agencies
- Establish Conventions for SAML usage
- Update NZSAMS & eGov profile
- Lab Implementation
- Work with Vendors
Questions?

Bill.Young@ssc.govt.nz

http://www.e.govt.nz/services/authentication