

Stronger Authentication in a Federated World

Bill Young
Government Technology Services
NZ State Services Commission

STATE SERVICES COMMISSION
Te Komihana O Ngā Tari Kāwanatanga



Quick Background of NZ Authentication

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

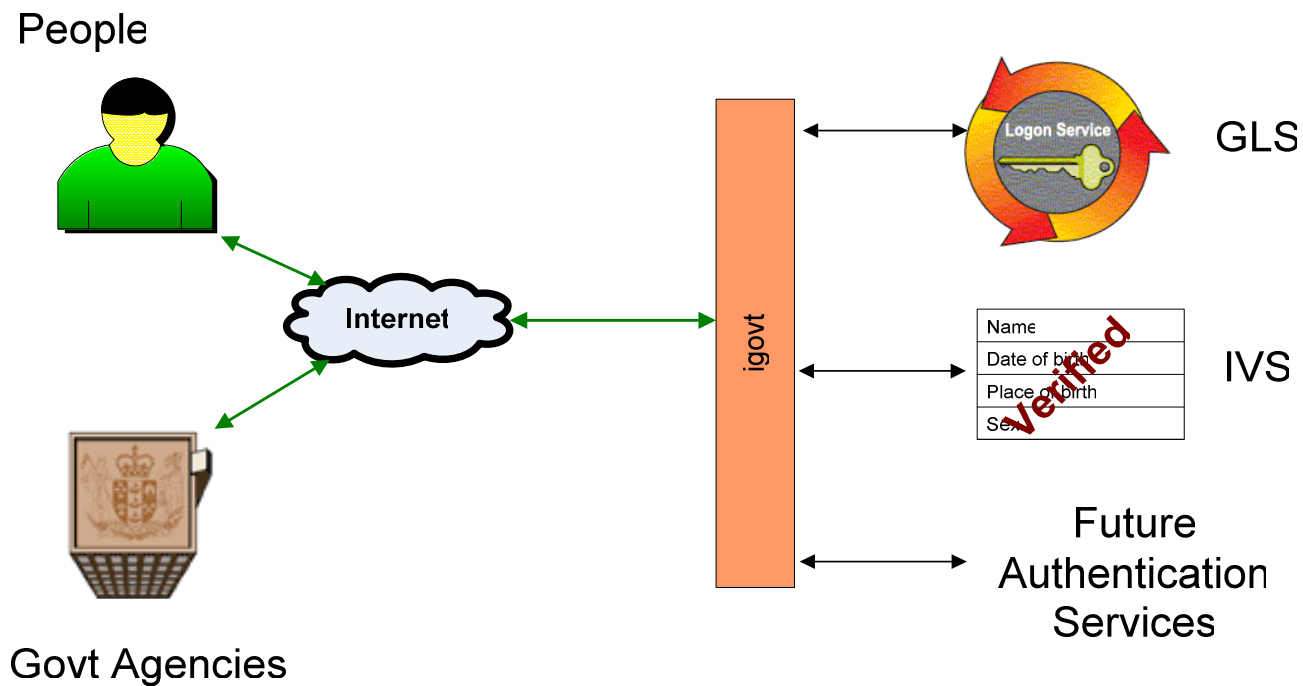


Our Big Drivers

- Privacy
- May not Disenfranchise any part of the Public
- Breadth of Scale in govt Departments



NZ AuthN & IdM Services



igovt

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)

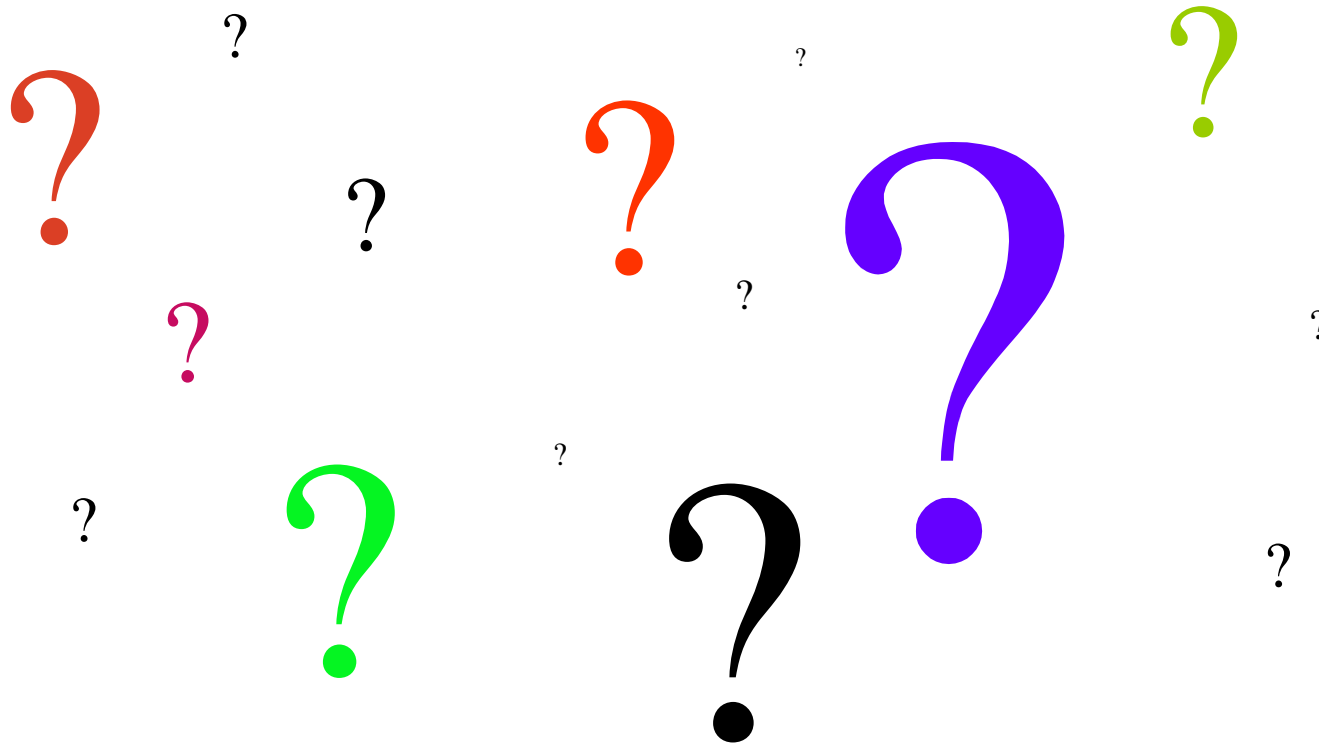
One Time Passwords (OTP)

- 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

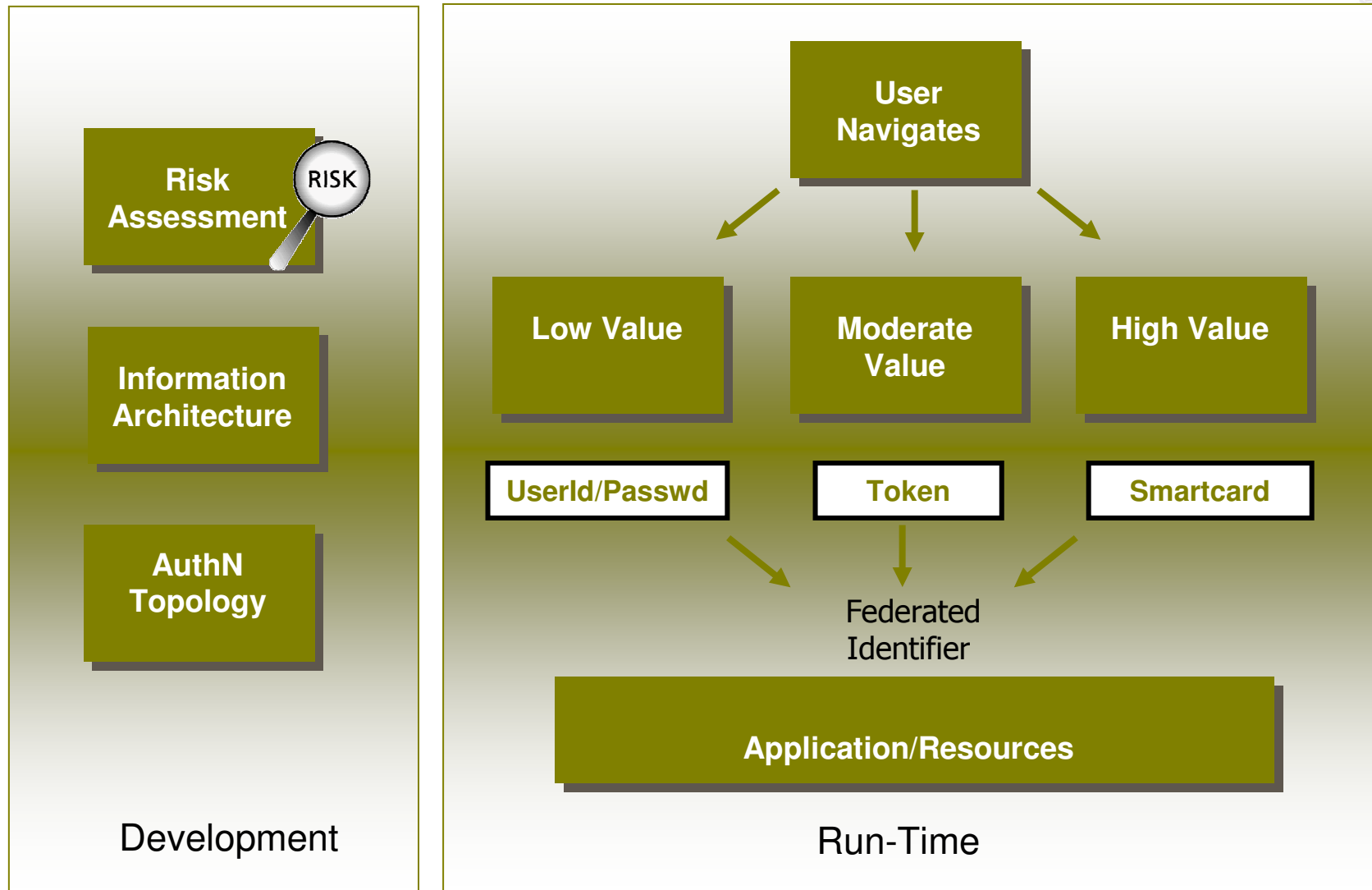


More Questions than Answers...

That's all fine, but...

**...how does it contribute to
a Risk-Based approach?**





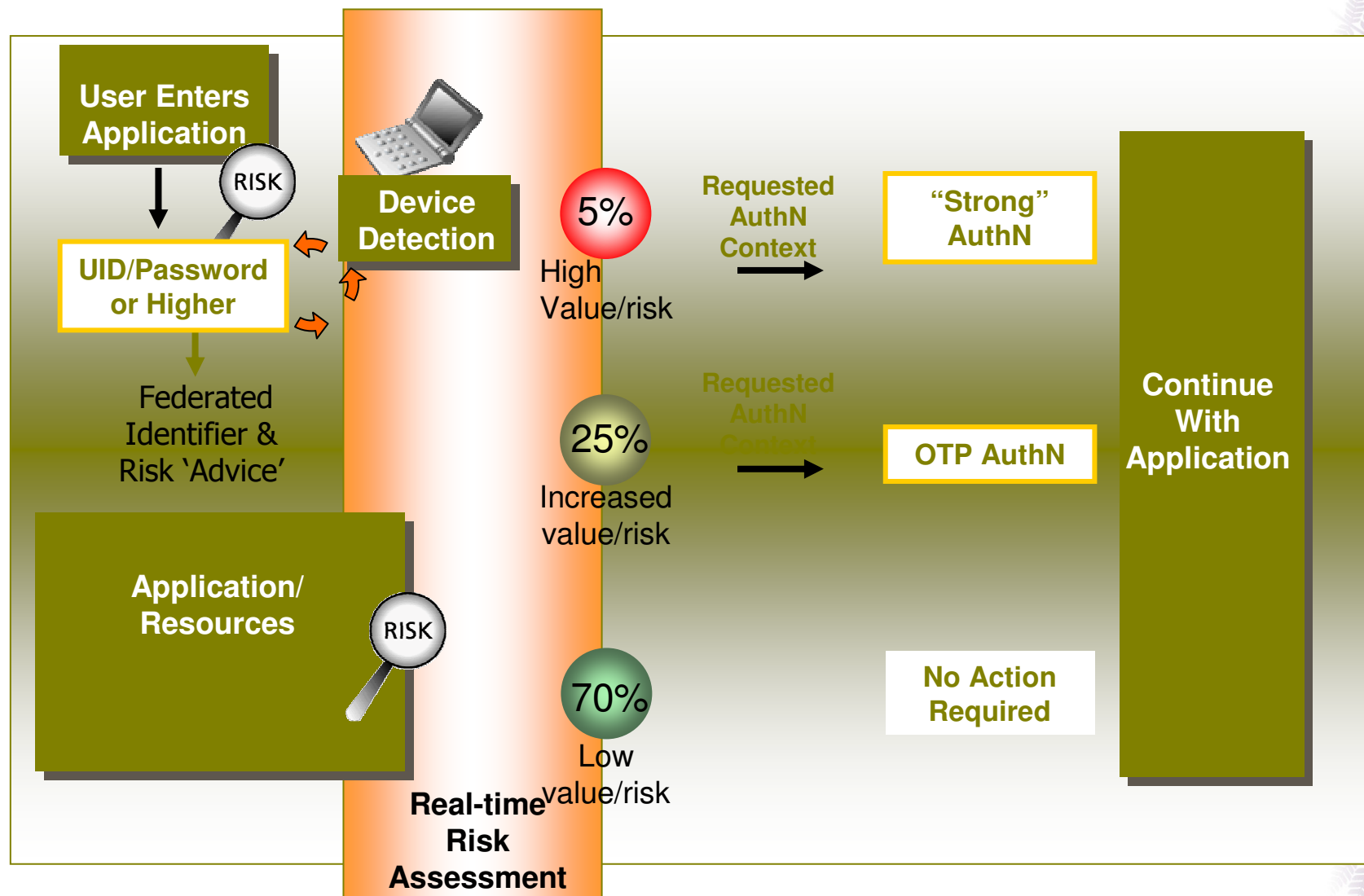
Context Sensitive Authentication

Definition:

*“Authentication based on
Real Time Risk Analysis”*



Context Sensitive Approach



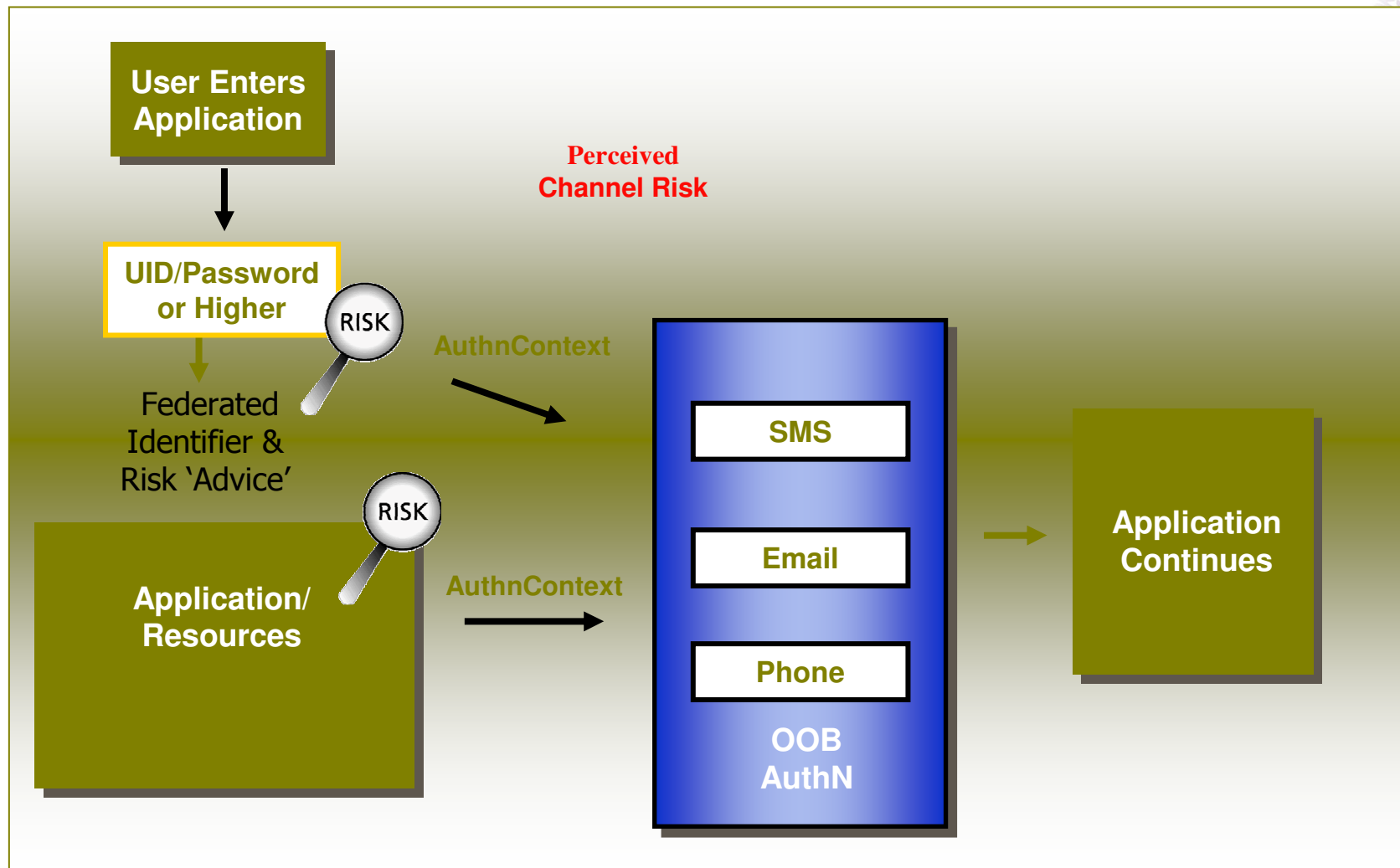
OOB Authentication

Definition:

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



Out of Band Authentication



Transaction Authentication/Verification

Definitions:

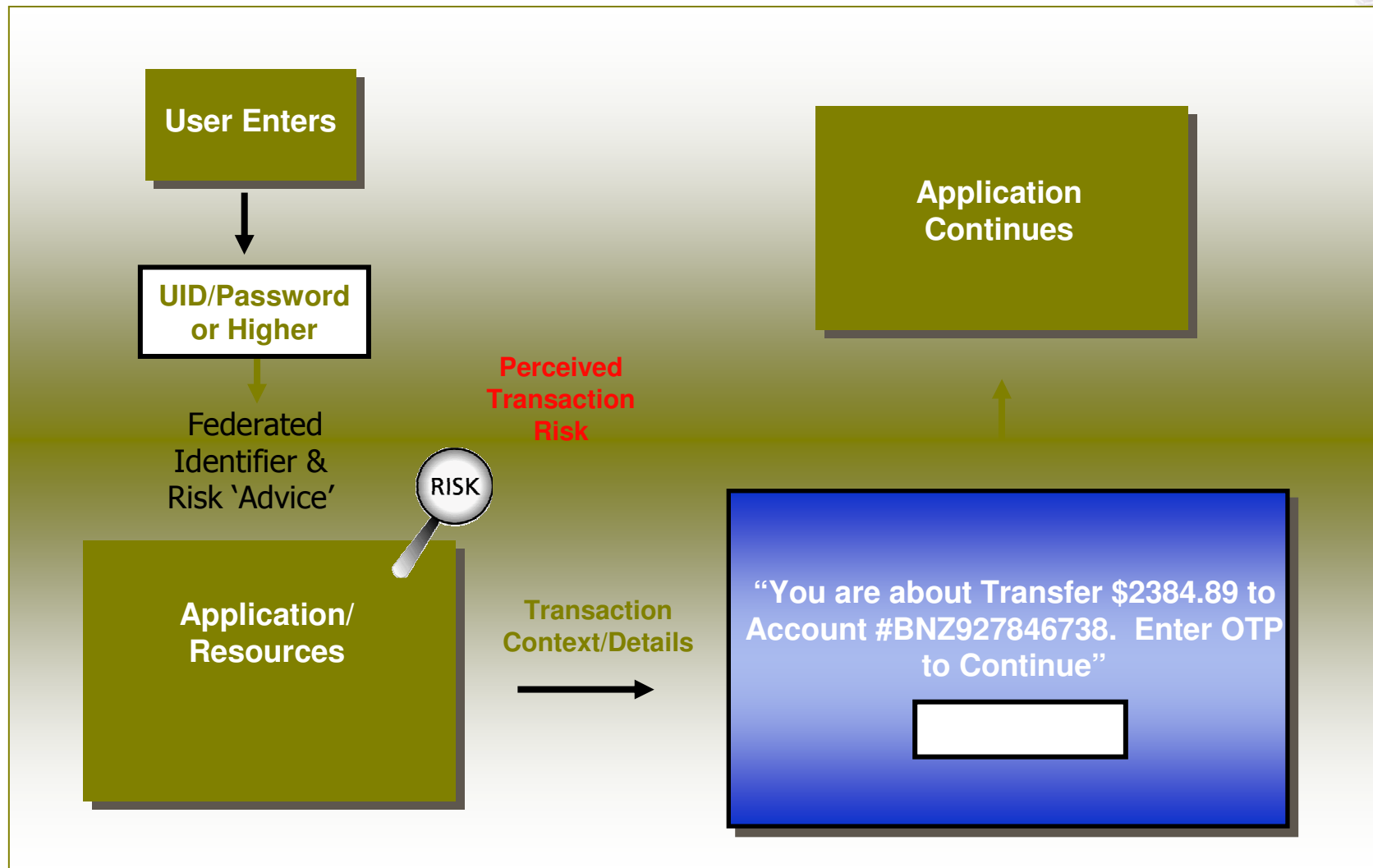
“Transaction Authentication Verifies that the Correct User is Requesting a Transaction”

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

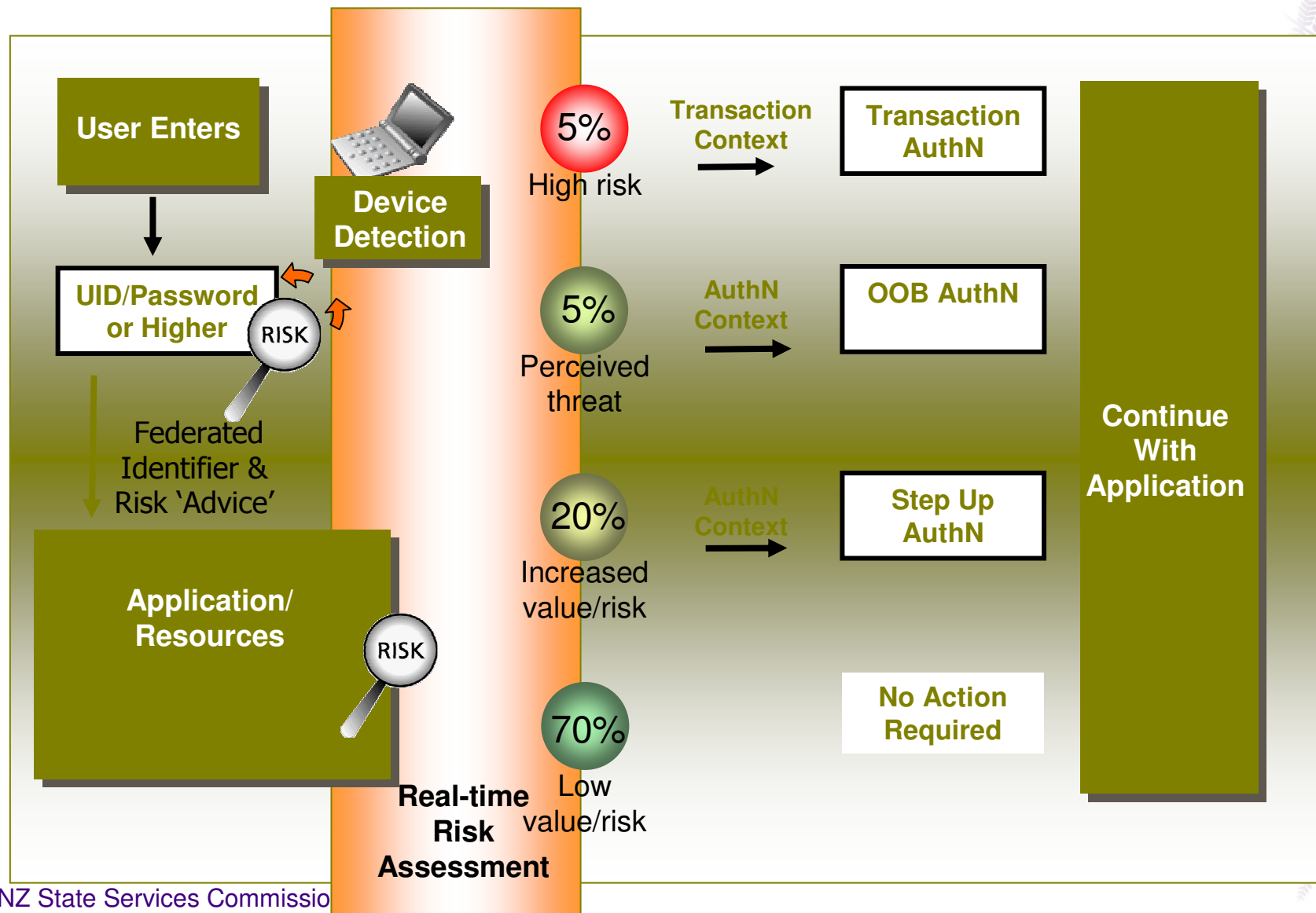
**I’m combining both under the term
“Transaction Authentication”**



Transaction Authentication



Putting it all Together



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

SAML Spec	Well Supported
Liberty Interop	Not Specified – Optional in US eAuth profile
eGov Profile	Supported
Vendor Support	Becoming Well Supported

Context Sensitive Authentication

Returning Risk Context to SP

SAML Spec	Well Supported
Liberty Interop	Not Specified
eGov Profile	Not Specified
Vendor Support	Mixed

OOB Authentication

Passing <Subject> to IdP

SAML Spec	Well Supported
Liberty Interop	Not Specified
eGov Profile	Not Specified or Restricted
Vendor Support	Unknown, but doubtful

Transaction Authentication

Transaction Details and Context

SAML Spec	Unanticipated – Some options available
Liberty Interop	Not Specified
eGov Profile	Not Specified
Vendor Support	Unknown, but doubtful

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>