canarie

Consent to Collaboration:

Balancing Security with Access for Optimal User Experience

Chris Phillips, CAF Technical Architect | April 25, 2016 | BCNET 2016

Agenda

- Overview (30 min)
  - Application and technology landscape
  - Identity principles in practice
- Diving into consent (30 min)
- Discussion (15 min)
- Break (15 min)
- Identity provider planning & walkthrough (60 min)
  - Hands-on work:
    - Clean installation
    - Upgrade
    - Maintenance
- Wrap-up & discussion (30 min)

Evolution of Identity Techniques

Application Centric IdM

- Services activated, but little interaction between them
- Applications have distinct userID/password pairs of their own

Centralizing Campus Directory & Sign-On

- Services are easier to turn on
- Users are using same password
- Campus SSO users sign in once
- Users sign in ‘once’
- Applications cannot see the user’s password

Federated SSO

- Faster service turn-up time – config and go
- Minimized attack/risk surface inherent in design
- Services outside your domain more easily enabled

Evolution of Identity Techniques

Application Centric IdM

- Services activated, but little interaction between them
- Applications have distinct userID/password pairs of their own

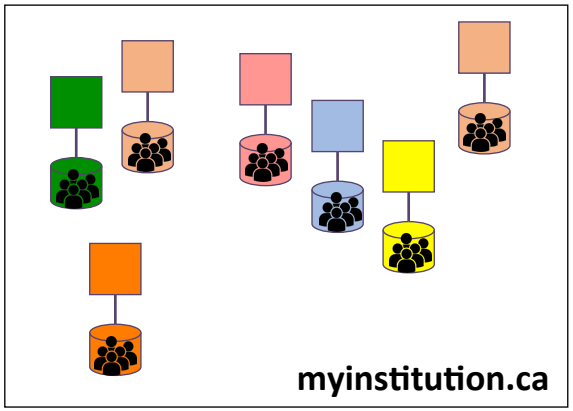
Centralizing Campus Directory & Sign-On

- Services are easier to turn on
- Users are using same password
- Campus SSO users sign in ‘once’
- Applications cannot see the user’s password

Federated SSO

- Faster service turn-up time – config and go
- Minimized attack/risk surface inherent in design
- Services outside your domain more easily enabled

Portfolio



Evolution of Identity Techniques

Application Centric IdM

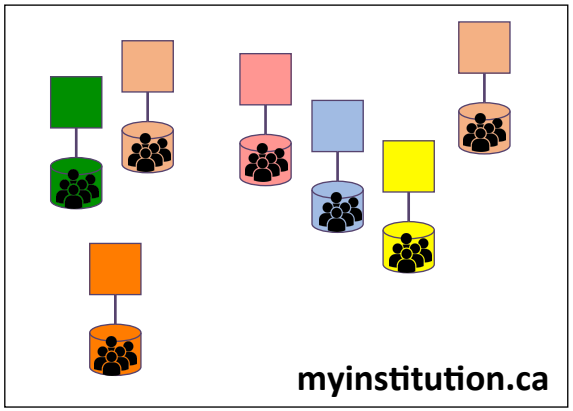
- Services activated, but little interaction between them
- Applications have distinct userID/password pairs of their own

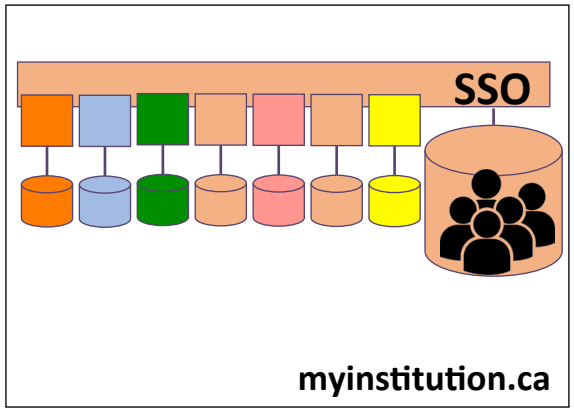
Centralizing Campus Directory & Sign-On

- Services are easier to turn on
- Users are using same password
- Campus SSO users sign in ‘once’
- Applications cannot see the user’s password

Federated SSO

- Faster service turn-up time – config and go
- Minimized attack/risk surface inherent in design
- Services outside your domain more easily enabled





Evolution of Identity Techniques

Application Centric IdM

- Services activated, but little interaction between them
- Applications have distinct userID/password pairs of their own

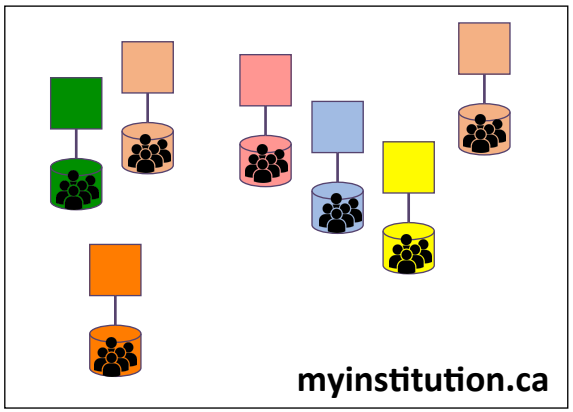
Centralizing Campus Directory & Sign-On

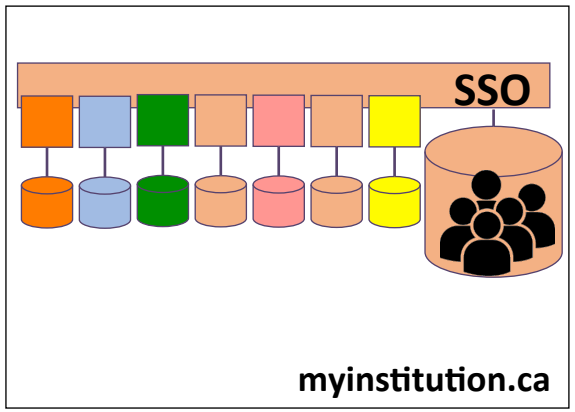
- Services are easier to turn on
- Users are using same password
- Campus SSO users sign in 'once'
- Applications cannot see the user's password

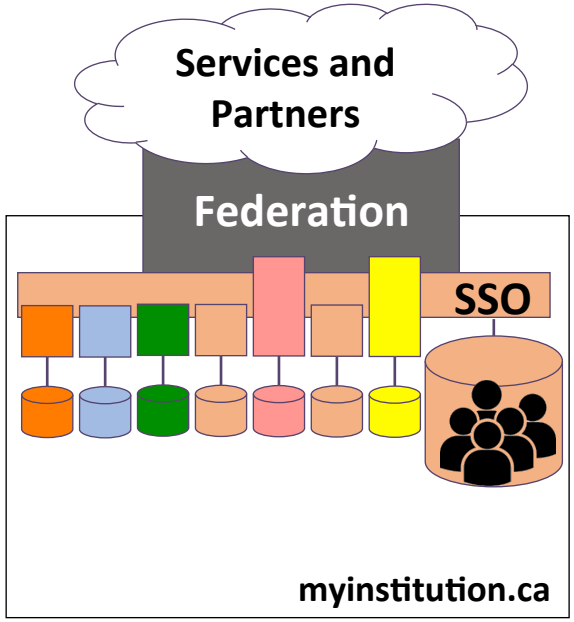
Federated SSO

- Faster service turn-up time – config and go
- Minimized attack/risk surface inherent in design
- Services outside your domain more easily enabled

Portfolio

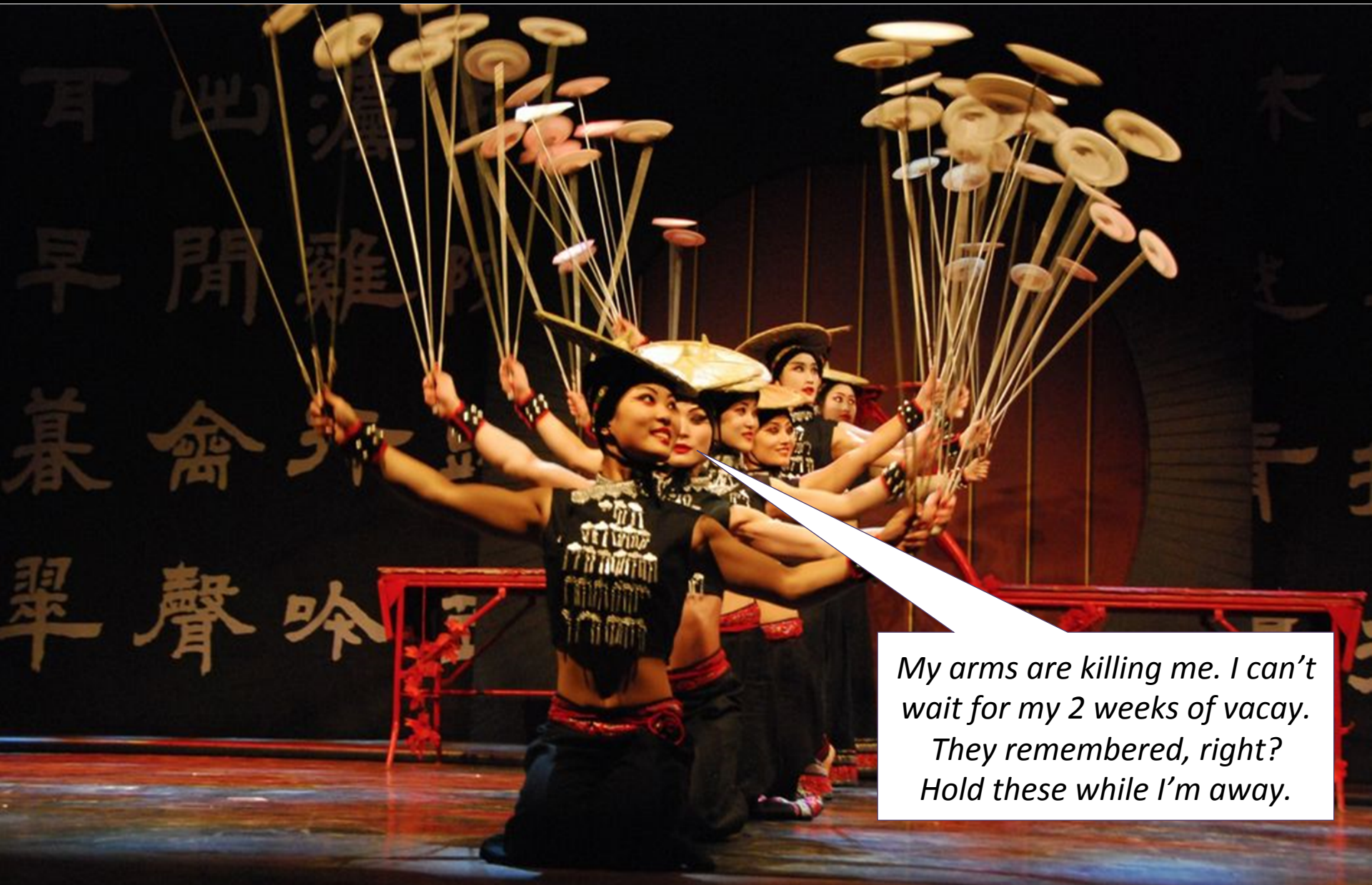






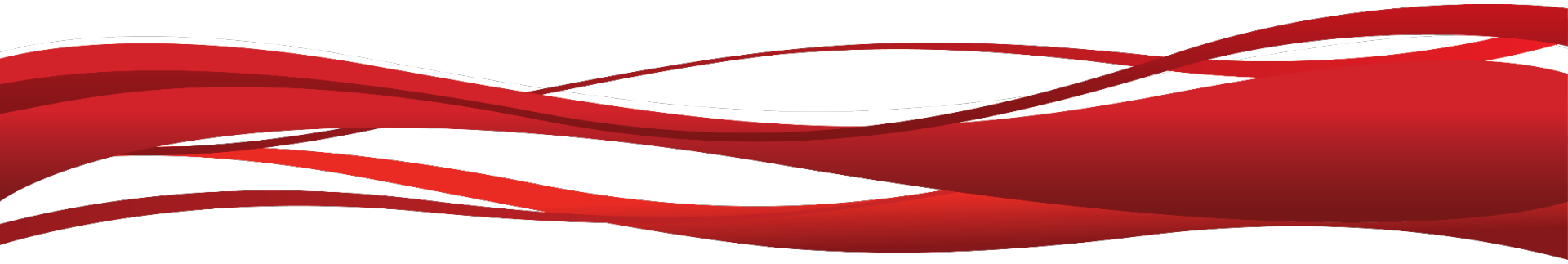
What delivering services feels like…

…it just doesn't scale up.

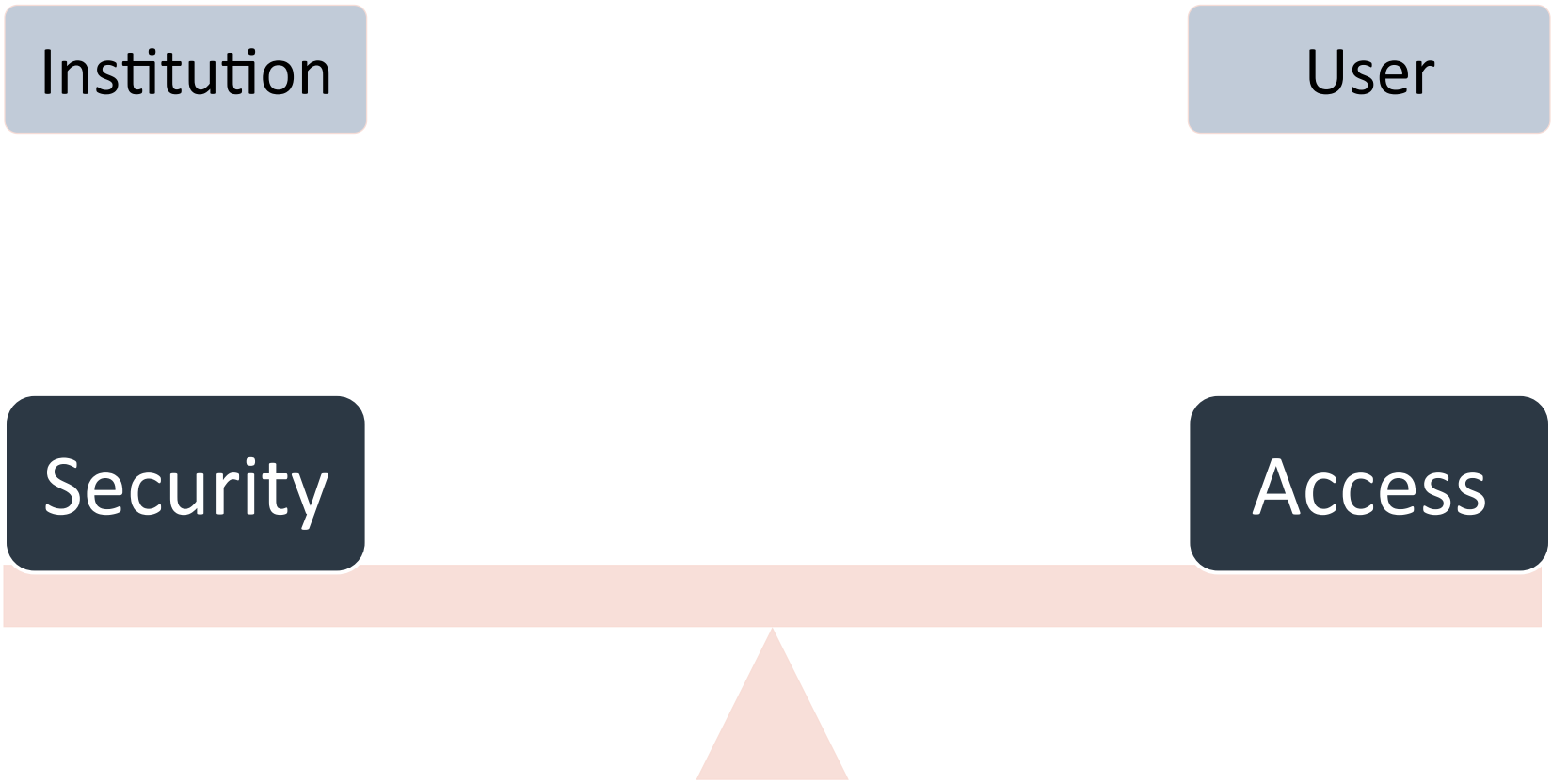


Don’t be mesmerized by spinning plates.

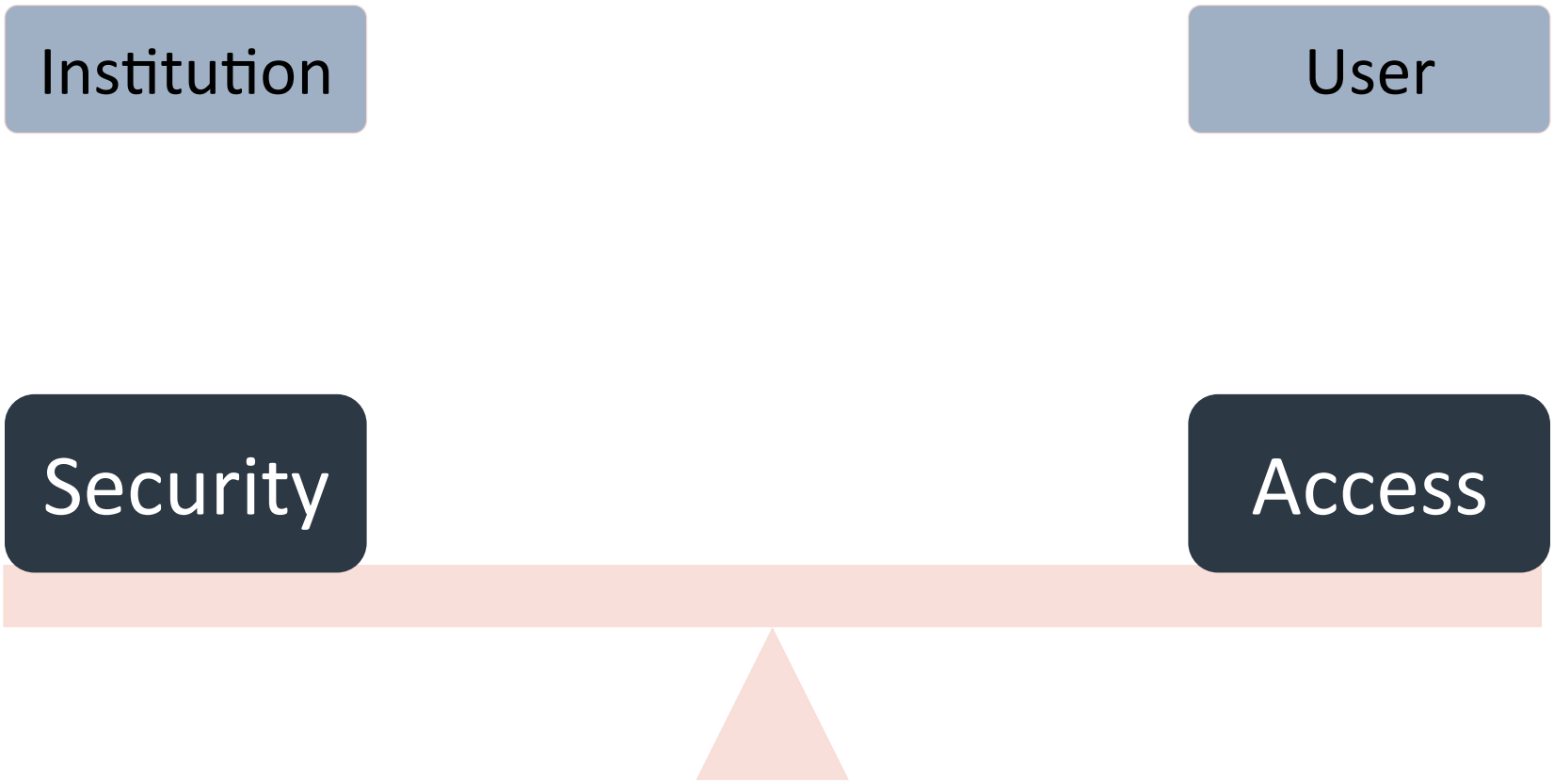
Reframing the Challenge

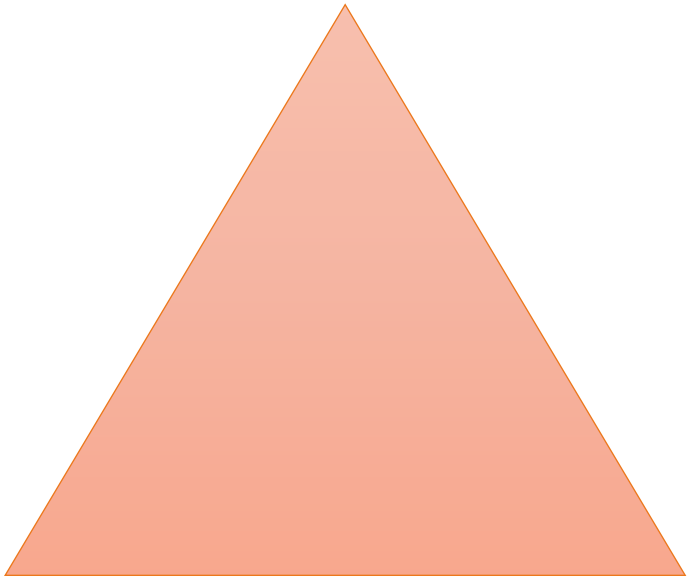


Reframing the Challenge

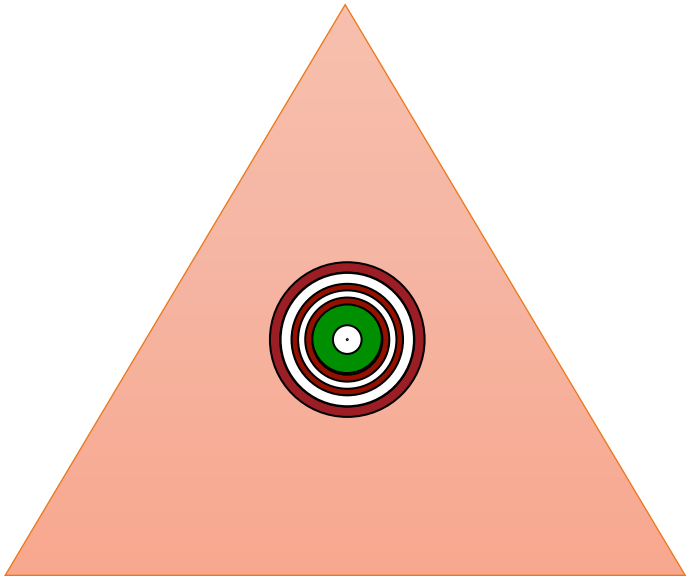


Reframing the Challenge





User eXperience (UX)

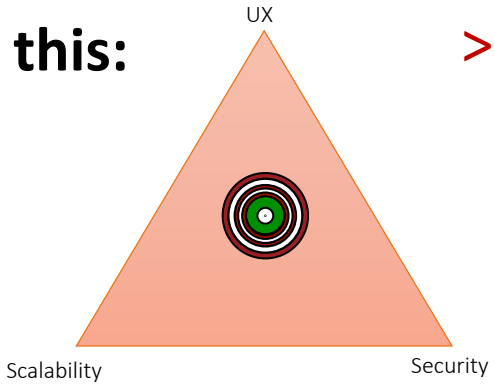


Scales by being easy to maintain & support

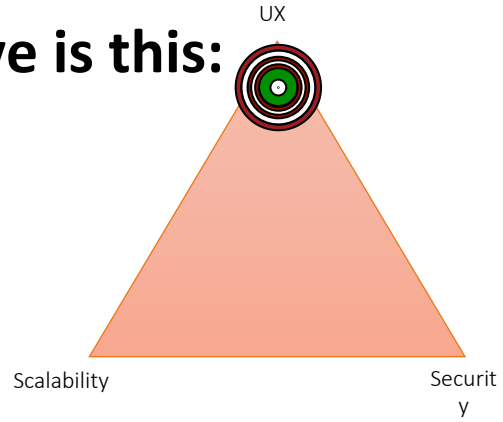
Safe and secure

No one is perfect

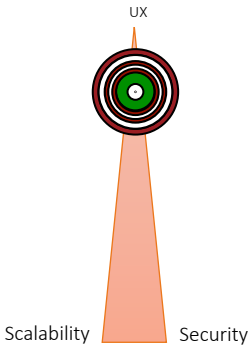
> IT wants this:



> User's drive is this:

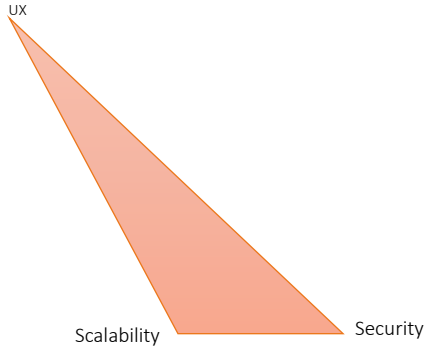


> We're left with this:



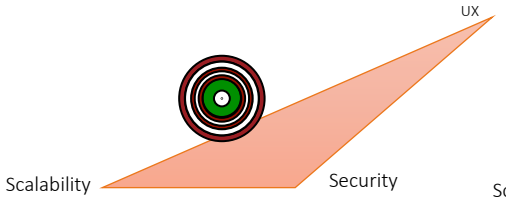
"It's a web app my department can't do without. My users love it. I run it from my machine under the desk. Didn't you know about it?"

The Christmas Tree



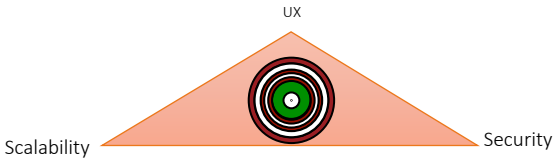
"I signed up for this service with my own funds; can I get a copy of the password hashes from you or drill a hole in the firewall to connect to LDAP so users can sign in?"

The Road of Good Intentions



"It's just a webserver with .htaccess and I share the password. When was the password last changed? A few years ago, why? Who has the password? Anyone from the conference, why?"

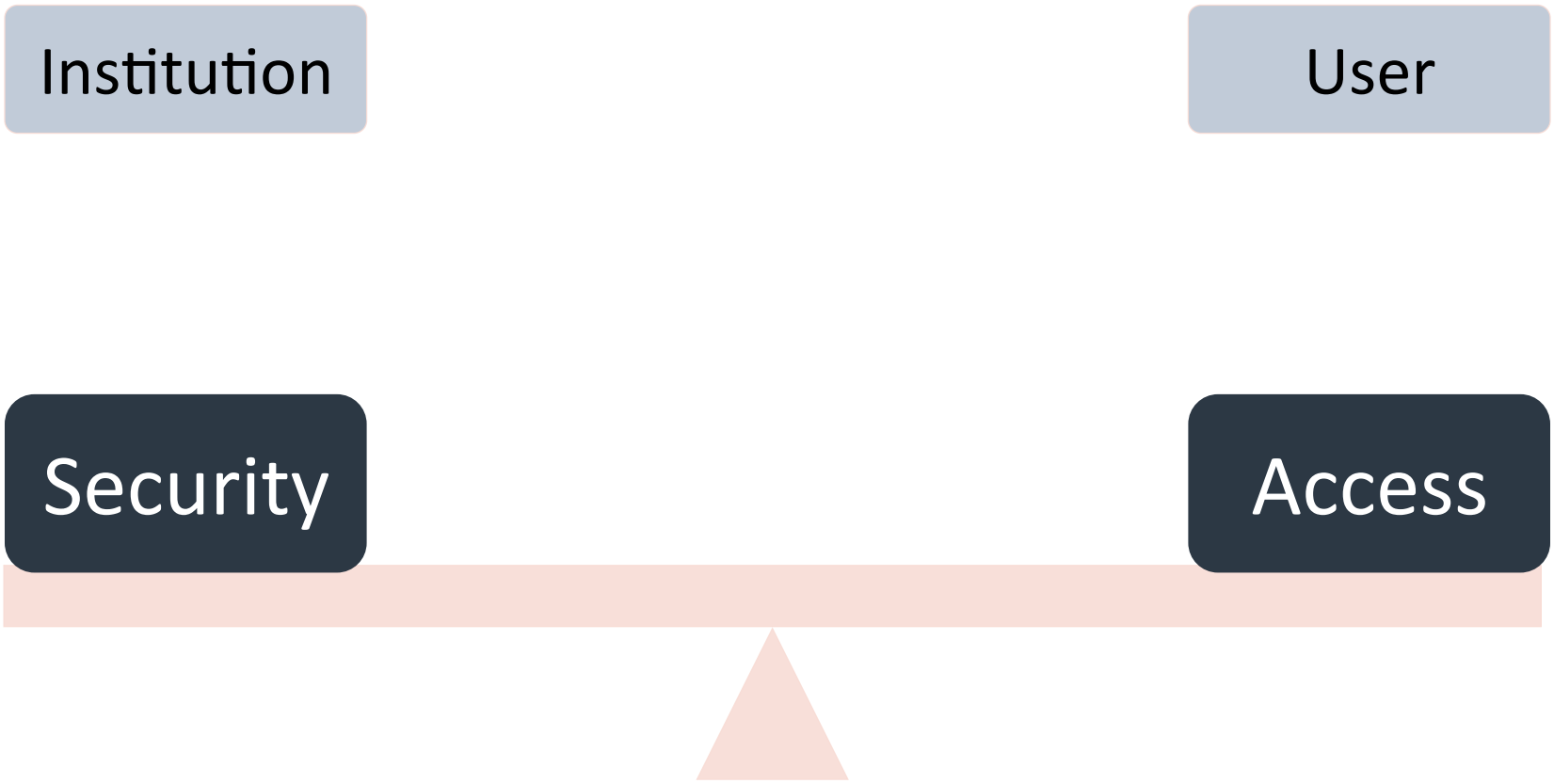
The Hitchhiker



"We have the service configured and registered but not a lot of uptake or still get questions about how to access instead of people just using it."

Middle of the Road

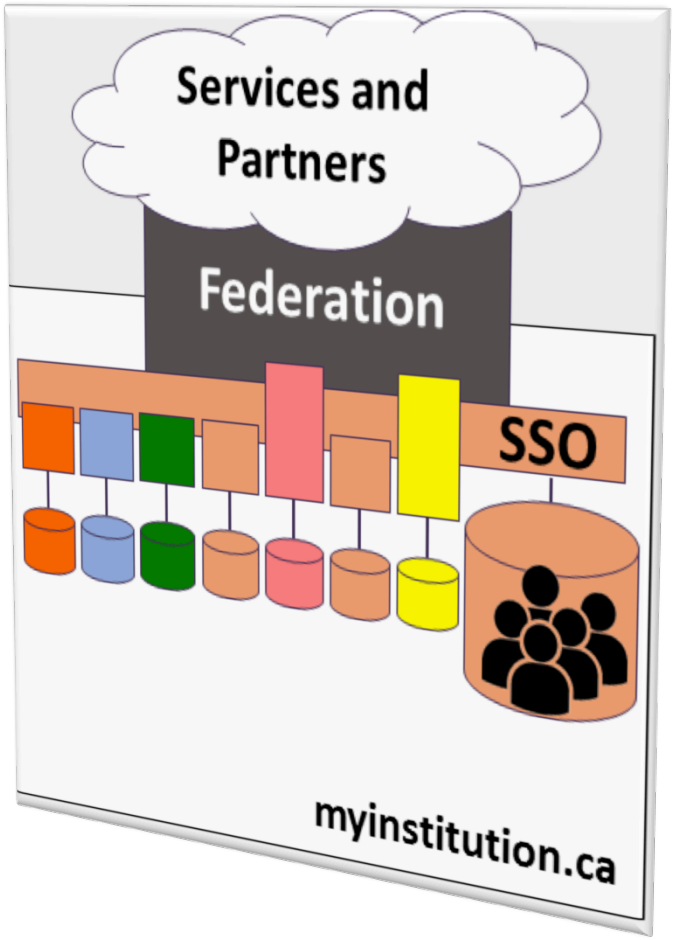
So What's Missing?



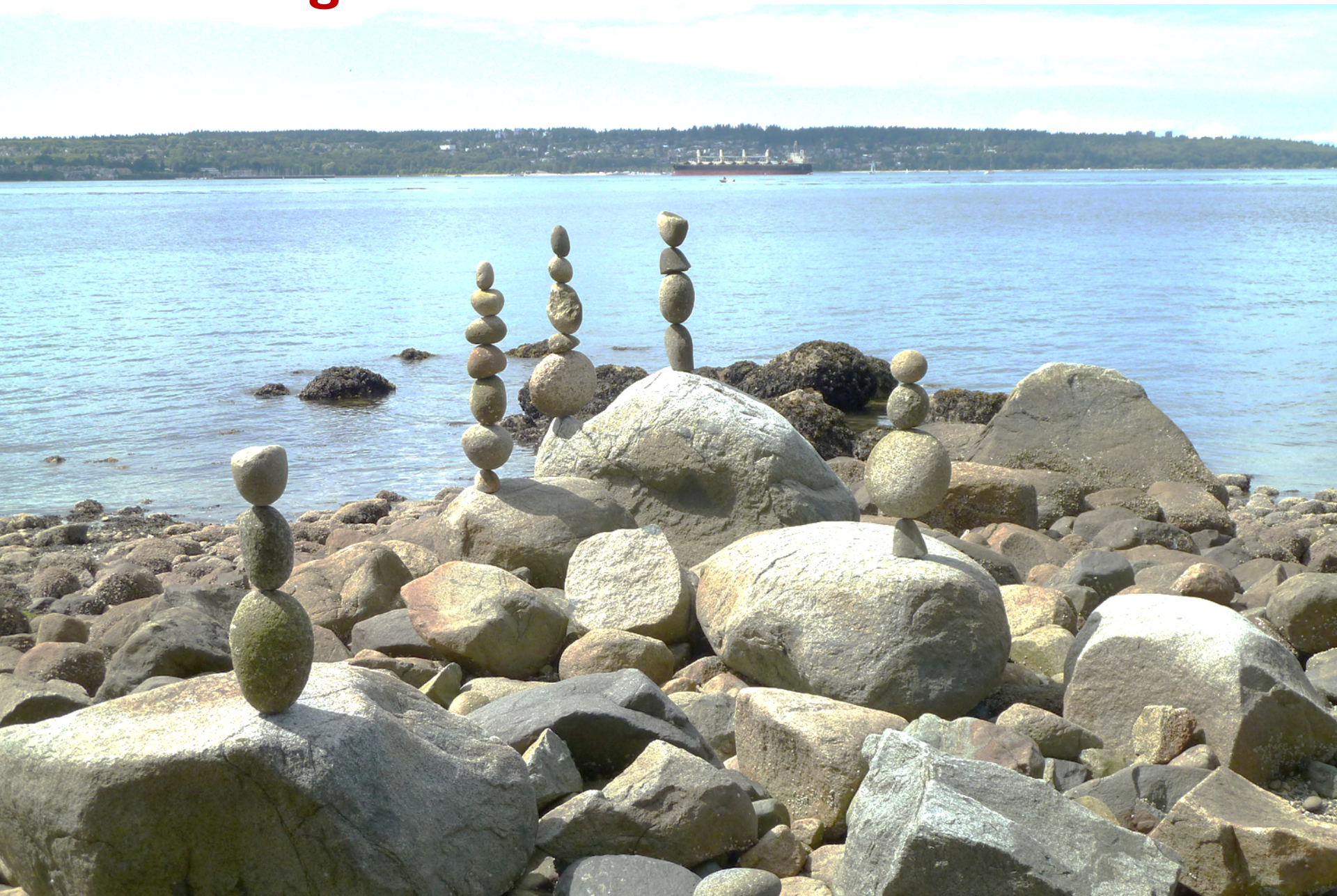
Attribute values are more important than the authentication itself. Without sufficient attributes, services cease to be of value.

Evolving the Conversation

- The infrastructure is there, but the attributes aren't
- Firewall-like behaviour today
  - Deny all and explicitly configure release
  - Doesn't scale
  - High friction to collaboration
  - Higher effort costs
- There's a better way



Enhancing Attribute Release



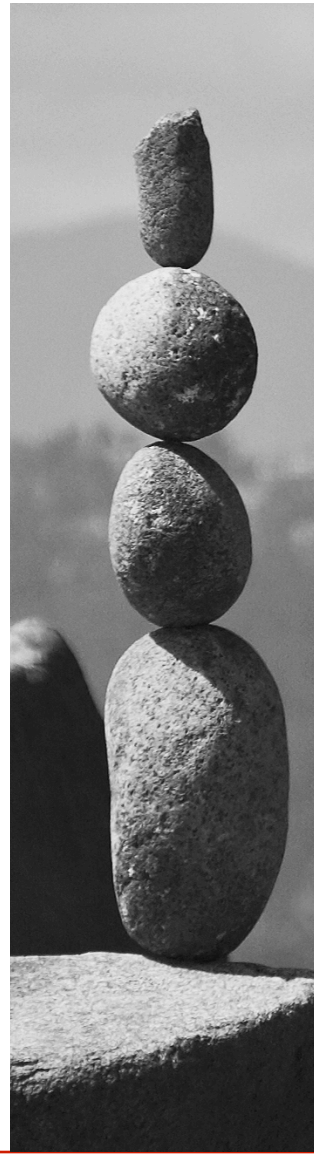
New Techniques

> Entity Categories

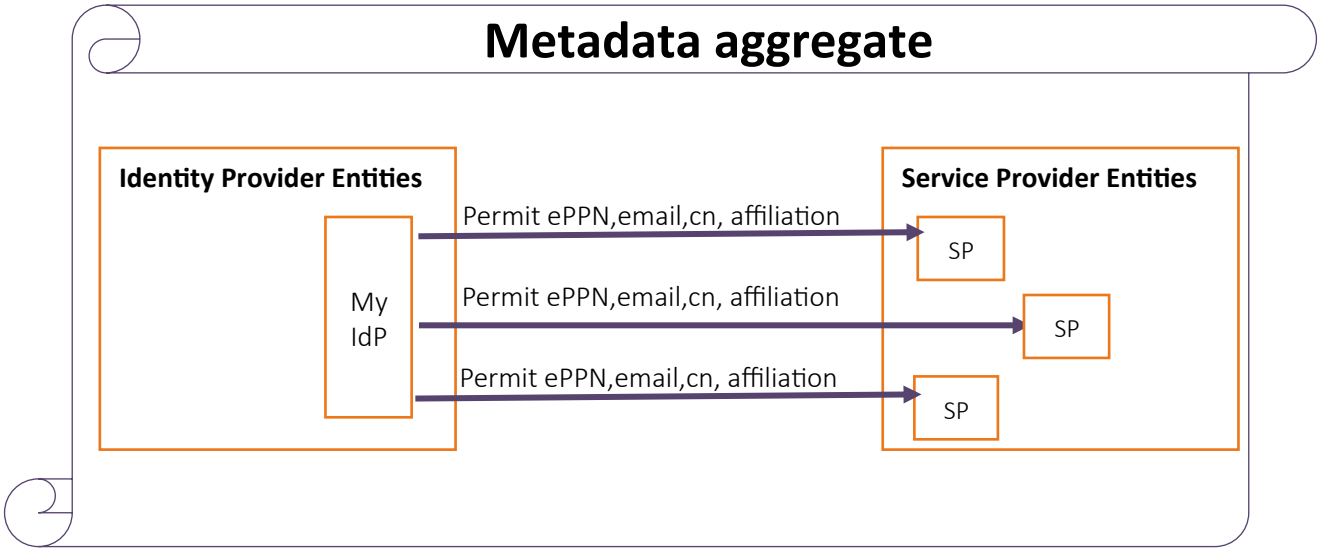
- A way to group federation entities that share common criteria
- obliged to conform to the characteristics set out in the definition of that category
- Facilitates IdP decisions to release a defined set of attributes to SPs
- Expressed as a SAML Attribute

> IdP-Configured User Consent

- Highlights data to end user
- Ability to ‘just turn it on’ out-of-the-box
- IdP operator has record of user consent



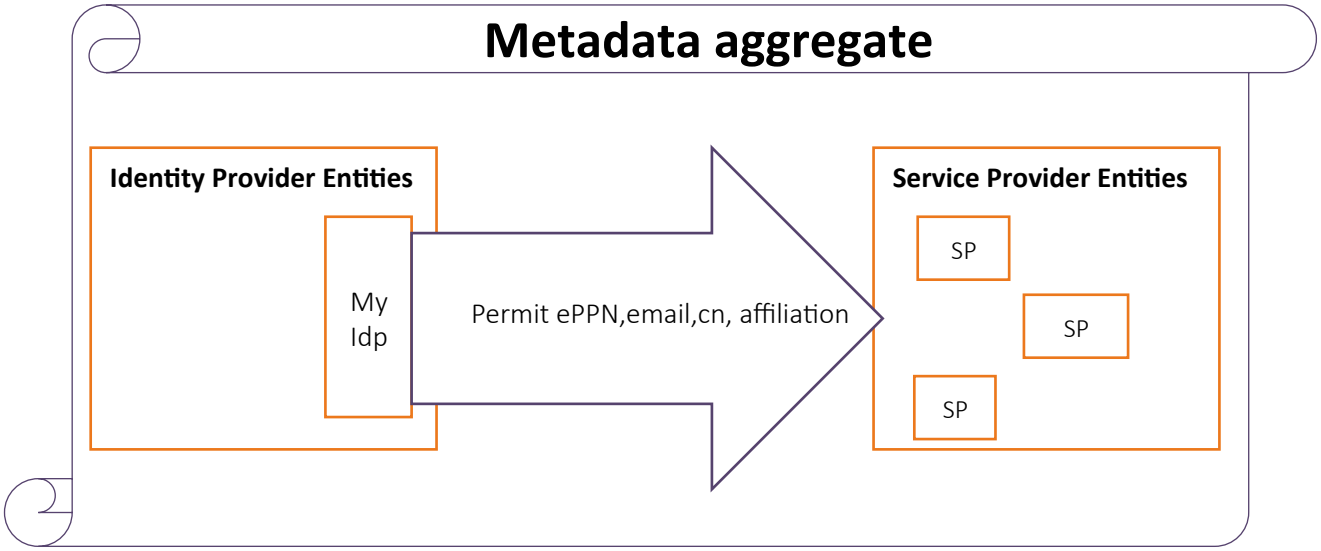
How Entity Categories Scale Attribute Release



> **Release Style A:** Classic service by service

- Create policy for each service you want to trust
  - 1:N entities
  - Fine grained, one time but higher effort

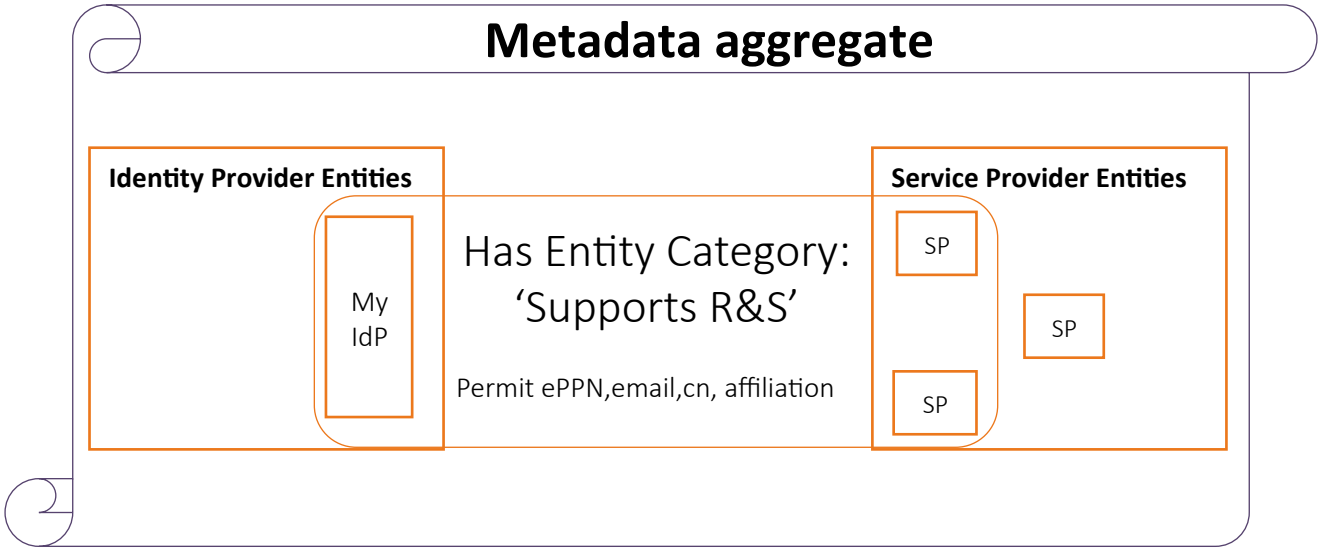
How Entity Categories Scale Attribute Release



> **Release Style B:** Classic release set to that which I trust

- Create ONE policy for ***entire*** aggregate
  - Permit attributes to flow regardless of entity
  - Works well for local campus federation where all entities are under one roof
  - Note this approach when we discuss consent!

How Entity Categories Scale Attribute Release



> **Release Style C:** Leverage entity categories

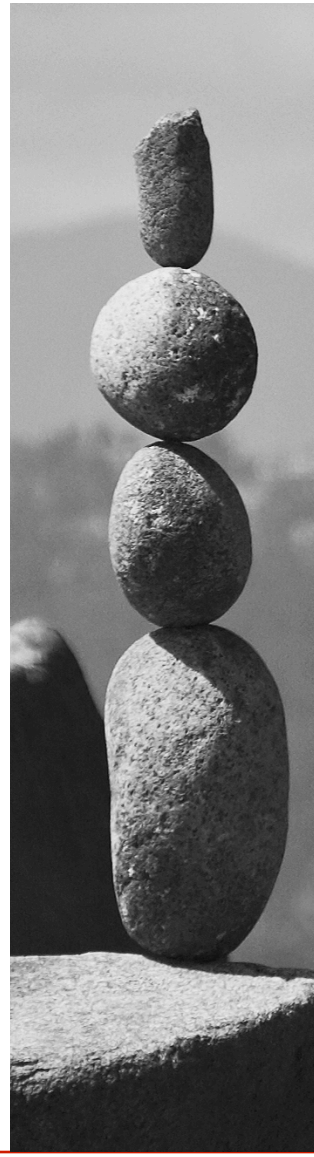
- Create policy for each category you want to trust
  - —1 category = many entities
  - —Worldwide usage so far: 87 SPs, 103 IdPs
  - —Policy is to the category criteria, NOT the entity identifier
  - —Equally thorough, less effort to maintain
  - —NO effort to enable new services who receive category; they just start working

Research and Scholarship Category

- Candidates for the Research and Scholarship (R&S) category are Service Providers that are operated for the purpose of
  - supporting research and scholarship interaction
  - collaboration or management, at least in part

- Examples of Service Providers:
  - collaborative tools and services such as wikis, blogs, project and grant management tools

- NOT-R&S example:
  - e-journal providers



Category Requirements

- Service Provider applies for membership from CAF and complies with the R&S registration criteria
  - Service enhances the research and scholarship activities of some subset of the registrar's user community
- Service Provider claims that it will not use attributes for purposes that fall outside of the service definition
- Using the Entity Category Support Attribute, an Identity Provider claims that it supports the release of attributes to R&S Service
  - An R&S SP can leverage this by filtering the list of IdPs on its chosen category

Technical Requirements

- Service Provider is a production SAML deployment
- Supports SAML V2.0 HTTP-POST binding
- Claims to refresh federation metadata at least daily
- Provides:
  - mdui:DisplayName
  - mdui:InformationURL
- Provides one or more technical contacts in metadata
- Provides requested attributes in metadata

Attributes

- Identity Providers are strongly encouraged to release the following bundle of attributes to R&S category Service Providers:
  - personal identifiers: email address, person name, eduPersonPrincipalName
  - pseudonymous identifier: eduPersonTargetedID
  - affiliation: eduPersonScopedAffiliation

- Minimum set:
  - eduPersonPrincipalName
  - mail
  - displayName OR (givenName AND sn)
  - (must use eduPersonTargetedID if PN is reassigned)

Applying Entity Categories in Practice

> On the IdP:

- Edit attribute-filter.xml
- Available on both Shibboleth v2 and v3
  - —V3 syntax shown

> On the SP:

- Only action is to request the assignment of the category by the registrar (CAF in Canada's case)

> In the metadata:

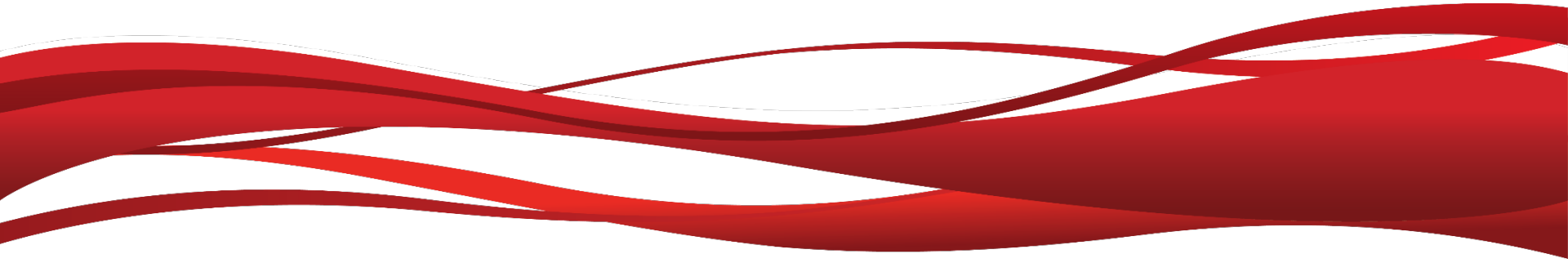
```
<AttributeFilterPolicy id="CAF-IdPInstaller-releaseToRandS">
    <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"
        attributeName="http://macedir.org/entity-category"
        attributeValue="http://refeds.org/category/research-and-scholarship" />

    <AttributeRule attributeID="displayName">
        <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false" />
    </AttributeRule>
    <AttributeRule attributeID="givenName">
        <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false" />
    </AttributeRule>
    <AttributeRule attributeID="surname">
        <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false" />
    </AttributeRule>
    <AttributeRule attributeID="email">
        <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false" />
    </AttributeRule>
    <AttributeRule attributeID="eduPersonPrincipalName">
        <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false" />
    </AttributeRule>
    <AttributeRule attributeID="eduPersonScopedAffiliation">
        <PermitValueRule xsi:type="AND">
            <Rule xsi:type="AttributeInMetadata" onlyIfRequired="false" />
            <Rule xsi:type="OR">
                <Rule xsi:type="Value" value="faculty" ignoreCase="true" />
                <Rule xsi:type="Value" value="student" ignoreCase="true" />
                <Rule xsi:type="Value" value="staff" ignoreCase="true" />
                <Rule xsi:type="Value" value="alum" ignoreCase="true" />
                <Rule xsi:type="Value" value="member" ignoreCase="true" />
                <Rule xsi:type="Value" value="affiliate" ignoreCase="true" />
                <Rule xsi:type="Value" value="employee" ignoreCase="true" />
                <Rule xsi:type="Value" value="library-walk-in" ignoreCase="true" />
            </Rule>
        </PermitValueRule>
    </AttributeRule>
</AttributeFilterPolicy>
```

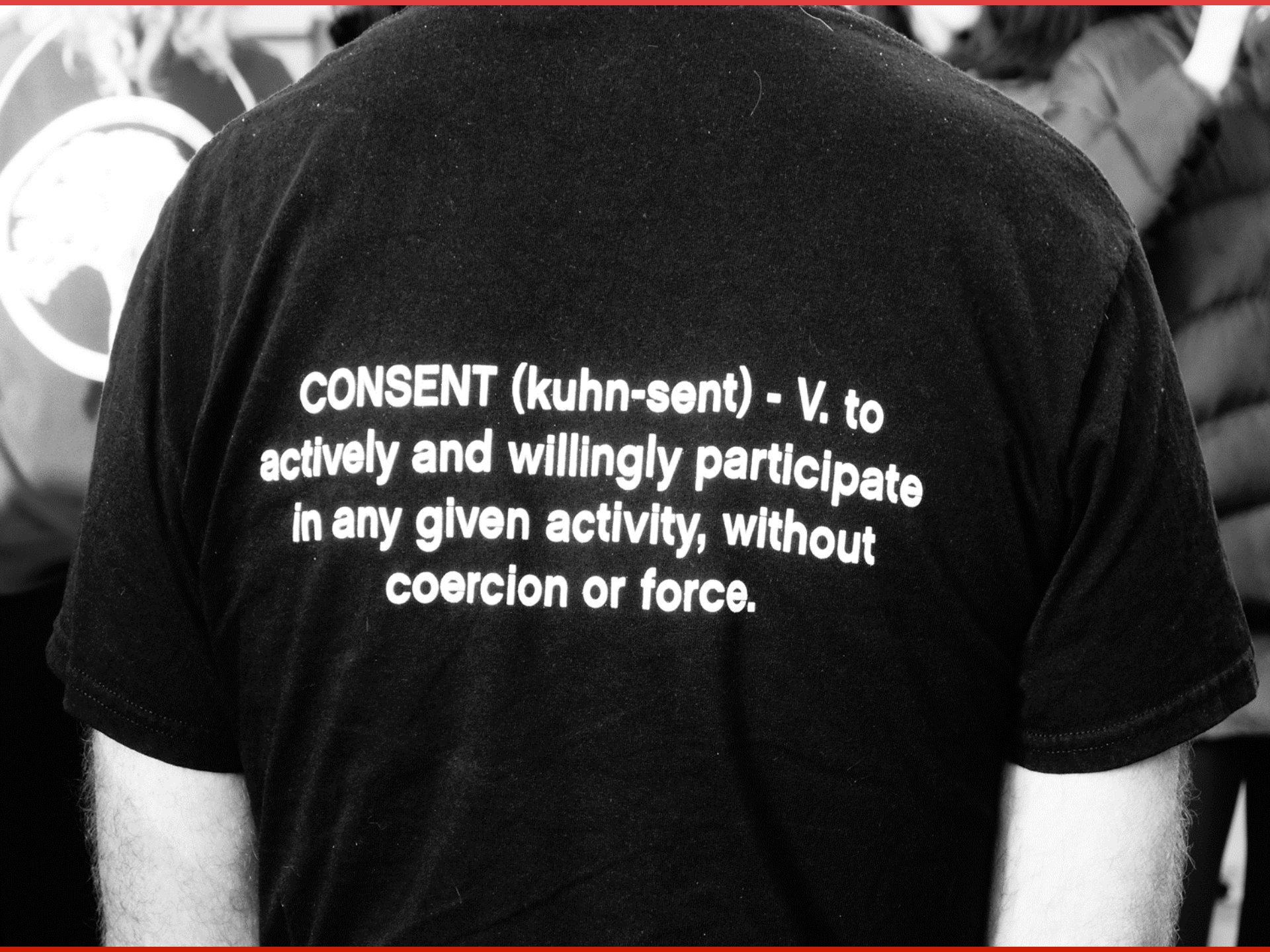
```
▼<mdattr:EntityAttributes>
  ▼<saml:Attribute Name="http://macedir.org/entity-category-support" NameFormat="urn:oas
    ▼<saml:AttributeValue>
       http://refeds.org/category/research-and-scholarship
     </saml:AttributeValue>
   </saml:Attribute>
 </mdattr:EntityAttributes>
</md:Extensions>
<md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
▼<md:Extensions>
```

Recap

- Entity categories enhance attribute release challenges
- Can be paired with other features like consent
- CAF:
  - Supports the Research & Scholarship category now
  - Encourages IdPs to to take advantage of the benefit
    - work through policy details and add category to IdP configuration ASAP

Becoming Consent Practitioners

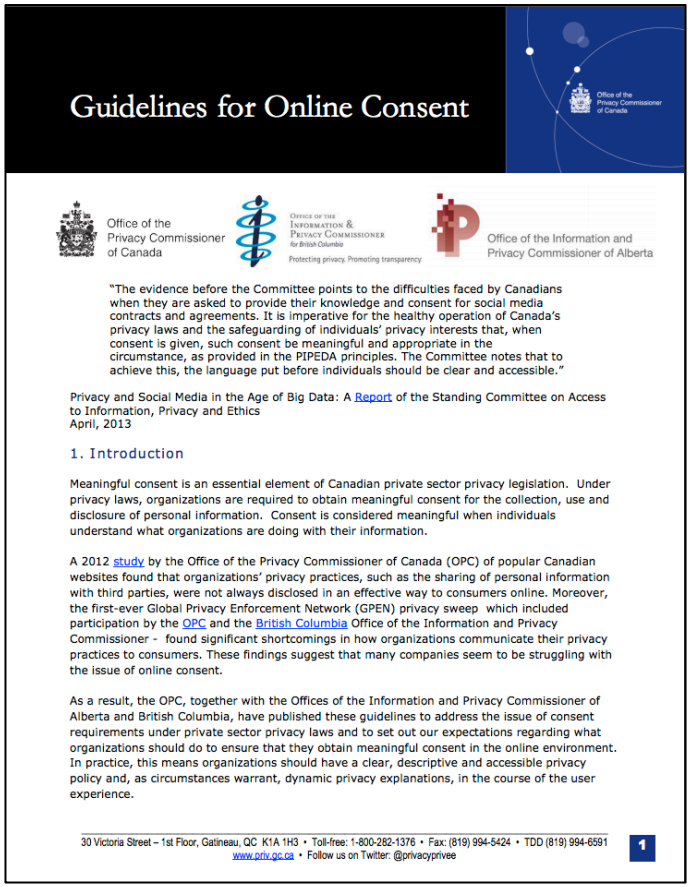



CONSENT (kuhn-sent) - V. to
actively and willingly participate
in any given activity, without
coercion or force.

Canadian Guidelines as our Rubric

> Key call outs*

- Reasonable purpose
- Conditions of Service
- Individuals must be informed
- Purposes for which organizations collect, use and disclose
- Obtaining consent
  - —does not release organizations from their other obligations under privacy laws, such as overall accountability, safeguards
- An organization is required to obtain the meaningful consent
  - —of an individual for the collection, use and disclosure of personal information.



Guidelines for Online Consent

Office of the Privacy Commissioner of Canada

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

Office of the Information and Privacy Commissioner of Alberta

"The evidence before the Committee points to the difficulties faced by Canadians when they are asked to provide their knowledge and consent for social media contracts and agreements. It is imperative for the healthy operation of Canada's privacy laws and the safeguarding of individuals' privacy interests that, when consent is given, such consent be meaningful and appropriate in the circumstance, as provided in the PIPEDA principles. The Committee notes that to achieve this, the language put before individuals should be clear and accessible."

Privacy and Social Media in the Age of Big Data: A Report of the Standing Committee on Access to Information, Privacy and Ethics
April, 2013

1. Introduction

Meaningful consent is an essential element of Canadian private sector privacy legislation. Under privacy laws, organizations are required to obtain meaningful consent for the collection, use and disclosure of personal information. Consent is considered meaningful when individuals understand what organizations are doing with their information.

A 2012 study by the Office of the Privacy Commissioner of Canada (OPC) of popular Canadian websites found that organizations' privacy practices, such as the sharing of personal information with third parties, were not always disclosed in an effective way to consumers online. Moreover, the first-ever Global Privacy Enforcement Network (GPEN) privacy sweep which included participation by the OPC and the British Columbia Office of the Information and Privacy Commissioner - found significant shortcomings in how organizations communicate their privacy practices to consumers. These findings suggest that many companies seem to be struggling with the issue of online consent.

As a result, the OPC, together with the Offices of the Information and Privacy Commissioner of Alberta and British Columbia, have published these guidelines to address the issue of consent requirements under private sector privacy laws and to set out our expectations regarding what organizations should do to ensure that they obtain meaningful consent in the online environment. In practice, this means organizations should have a clear, descriptive and accessible privacy policy and, as circumstances warrant, dynamic privacy explanations, in the course of the user experience.

30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

1

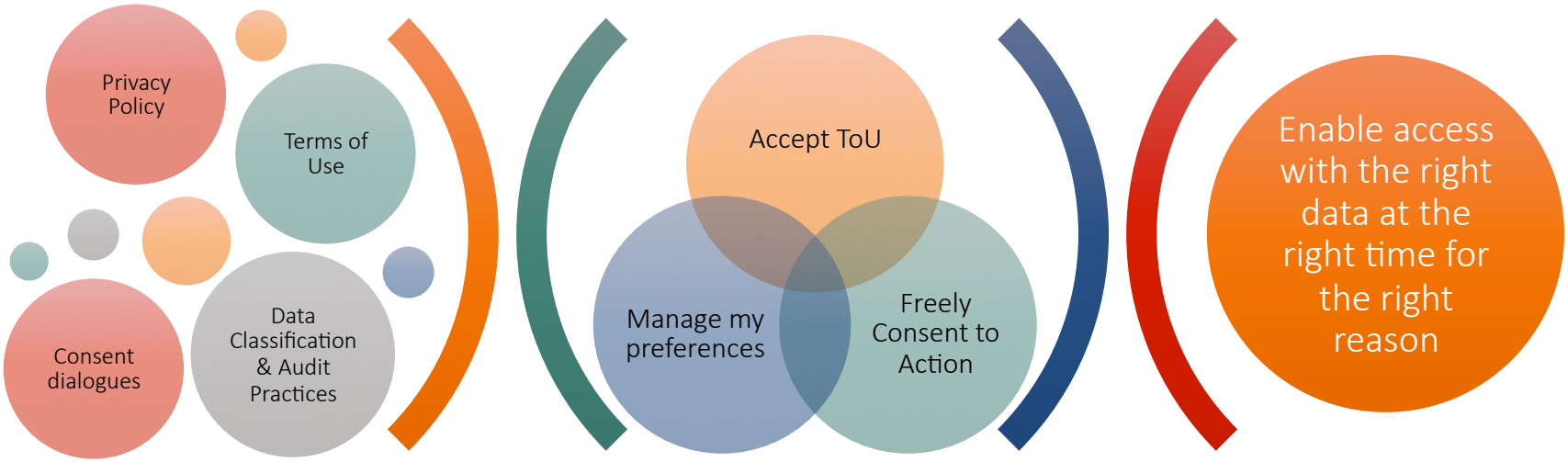
** Disclaimer: I'm not a privacy officer, and don't play one on TV either. Consult locally and engage early.*

https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_e.asp

It is good practice for organizations to put in place procedures for individuals to provide consent, and to retain proof that consent has been obtained.

Situations may arise where organizations may need to demonstrate that they have obtained consent, and having proof of consent built into a documented process will help accomplish that.

"The mechanics of online consent" section
https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_e.asp

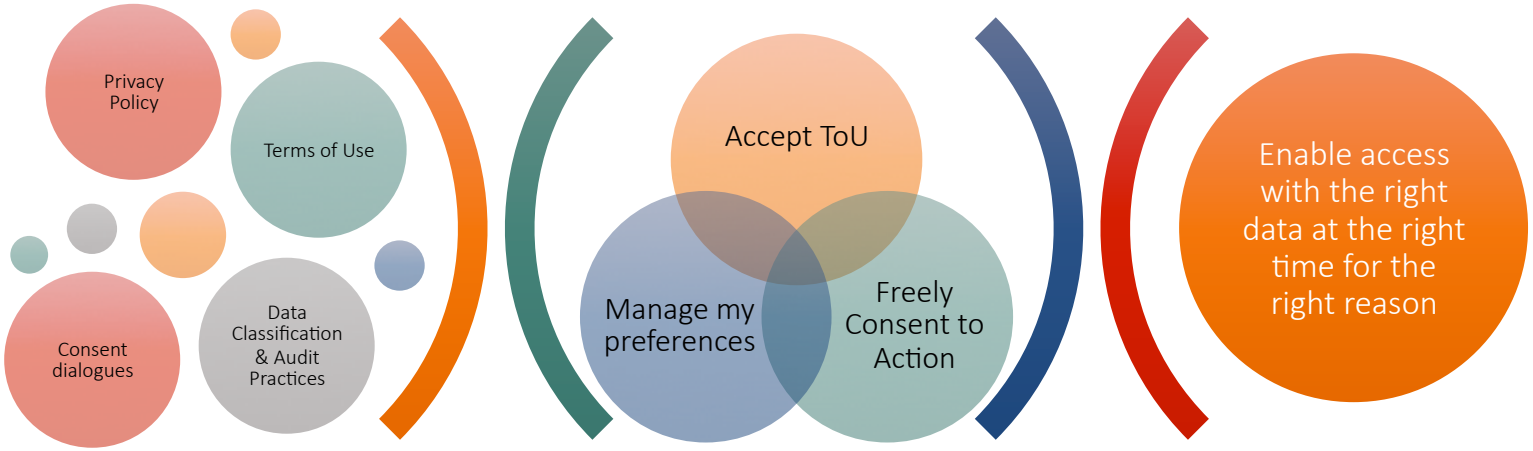


Say What you Do

Be Part of the Process

Do What you Say

Who's Responsible and Accountable?



Say What You Do | **Be Part of the Process** | **Do What You Say**

The Institution

The User

The Institution

Solution Fit Checklist

The Institution

> Privacy Policy in place?

> Terms of Use or Account Use Policy in place?

> Consent enabled?

> Audit trail available?

> Data Classification pass completed?

> Enabling access with the right data at the right time for the right reason?

The User

> Knows and Accepts Terms of Use?

> Can freely consent where possible?

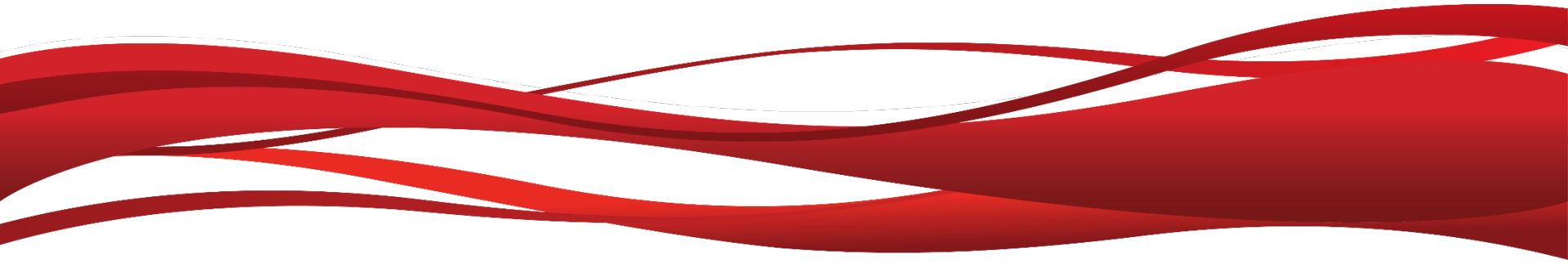
> Can manage preference somehow?

Technology Options for Consent Deployment

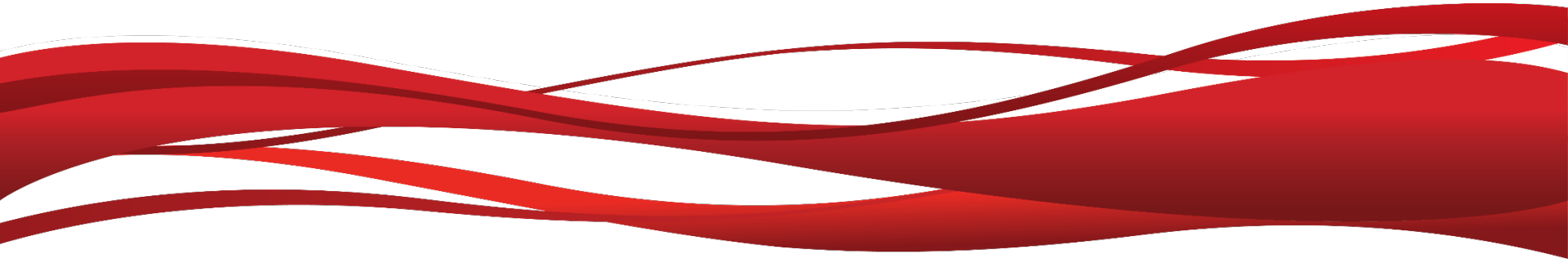
- No Change
  - Existing practices of idp controlled attribute release
  - Rely on pre-existing user agreements and privacy policy
- Consent for services
  - Easiest to enable and out of the box ready
  - Customizable
- Consent with Terms of Use by Service Provider
  - Customizable
  - Configurations: one ToU for all services, or per service
- Consent by audience
  - Configurable but a bit higher complexity
  - E.g. show consent for users with affiliation = student, otherwise no consent dialogs

Full details: https://wiki.shibboleth.net/confluence/display/IDP30/ConsentConfiguration

Interactive Segment



Demo of Sample Installation




TIME FOR A BREAK

Chris' SPEAKERS NOTES
new features of the Shibboleth version 3 Identity Provider will be demonstrated

> A walk through of the file structure?

> Common activities

> Updating certificates

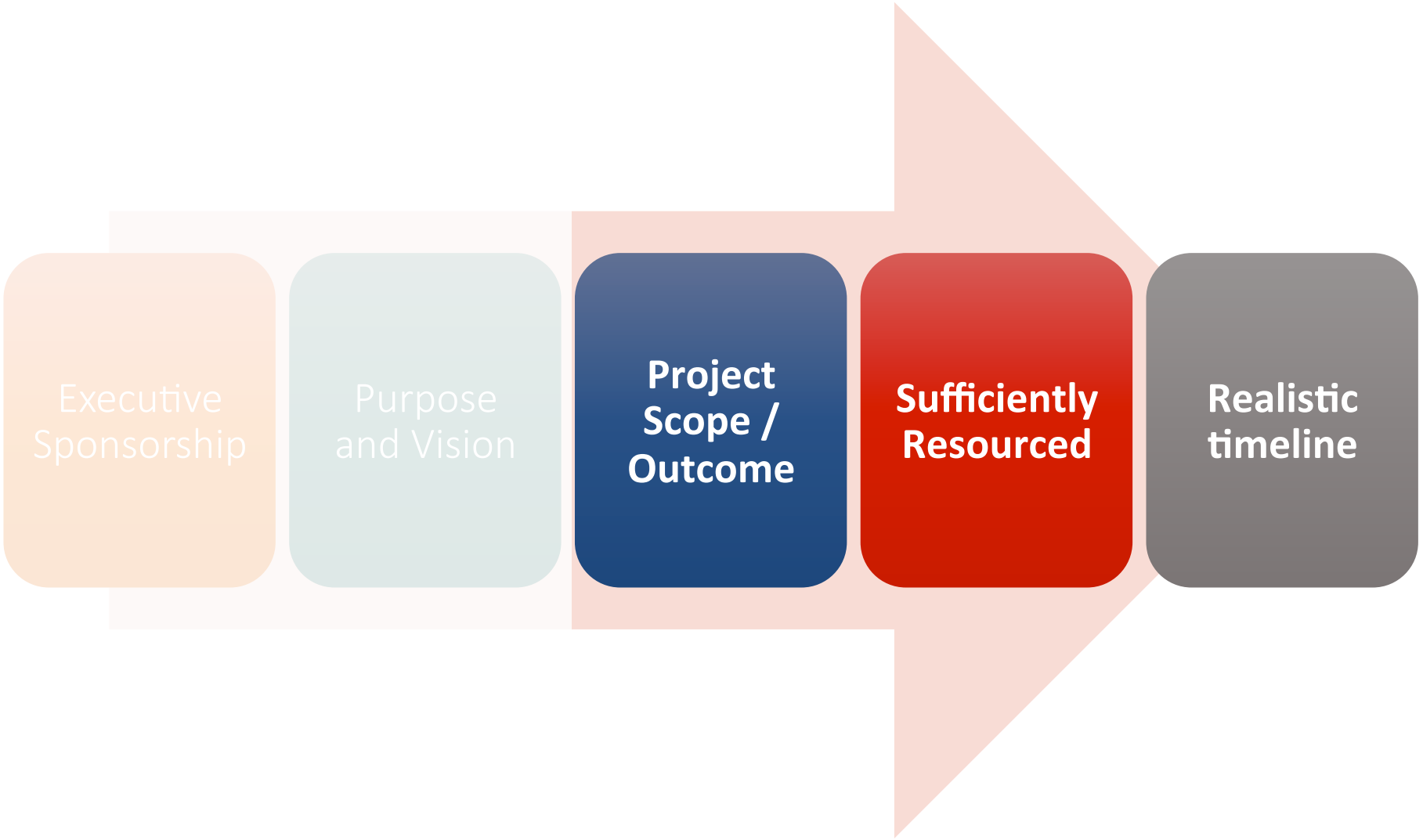
> Easier UI customization practices
- Customizing login page
- Customizing consent page

> Improved installation and upgrading for the latest version of the Shibboleth Identity Provider.

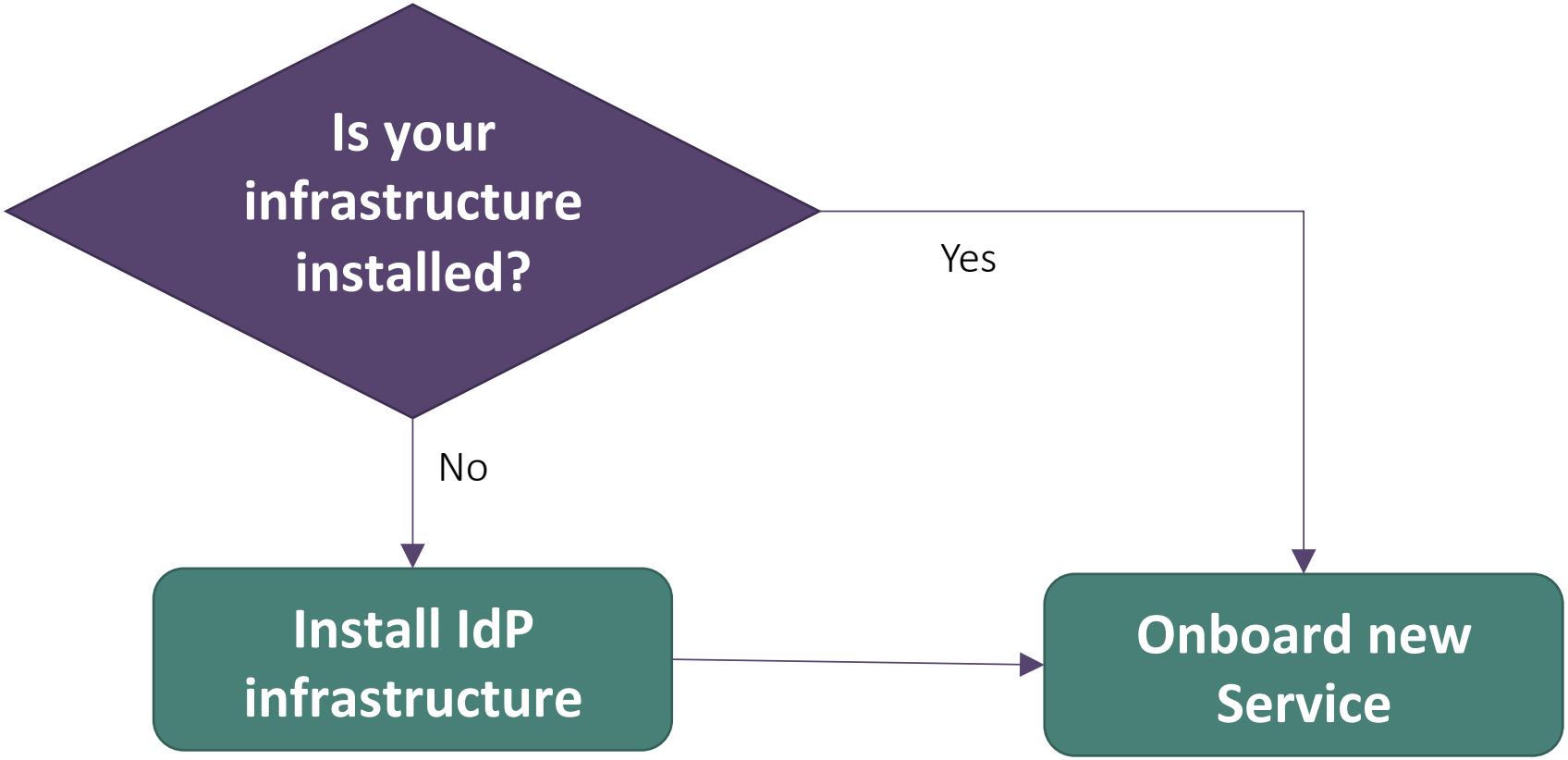
> New installations of the V3 software will also be discussed.
- Do an IdP Installer version

> An upgrade/installation plan to take home
- Checklist derived from idp installation work

Success Factors



Typical Project Scope and Path



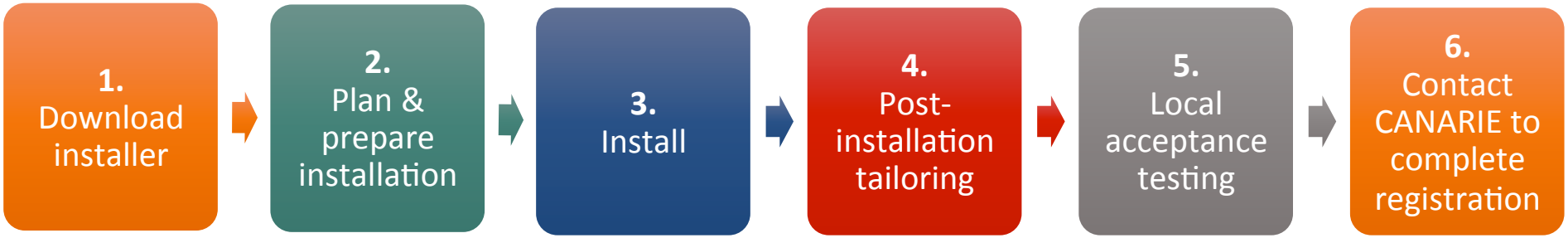
- Use CANARIE tools for fastest install
- Infrequent activity
- Usually done before services

- Leverages existing integration paths
- Favours configuration over customization
- Most frequent project activity

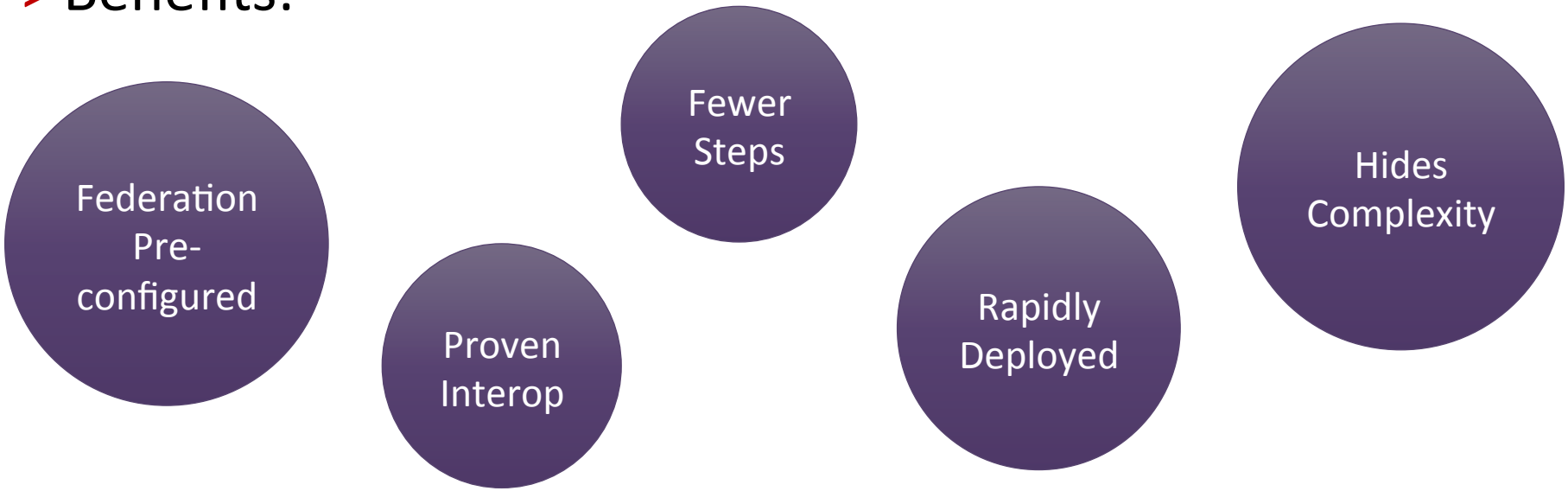
Why?

- Evolved approach to better match campus IT reality
- Reduced cost/effort to be CAF participant
- Simplifies CAF installation experience
- Easier day to day operations

Installation Process

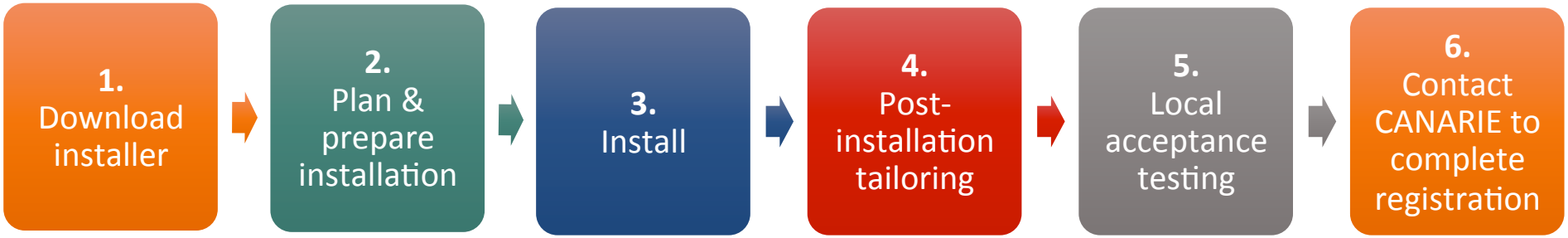


> Benefits:

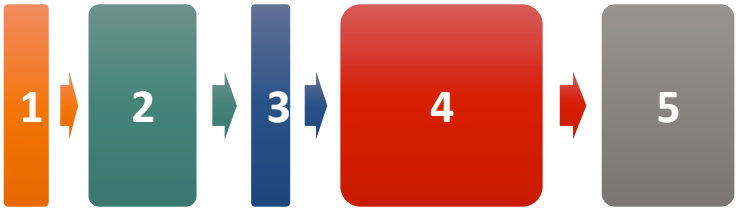


Automation makes things faster.

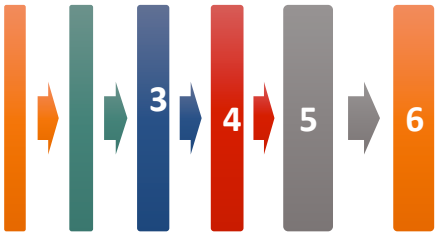
Baseline



1st time through installation (testing)



2nd & subsequent times through installation (production)



http://bit.ly/idpinstaller

Planning your time

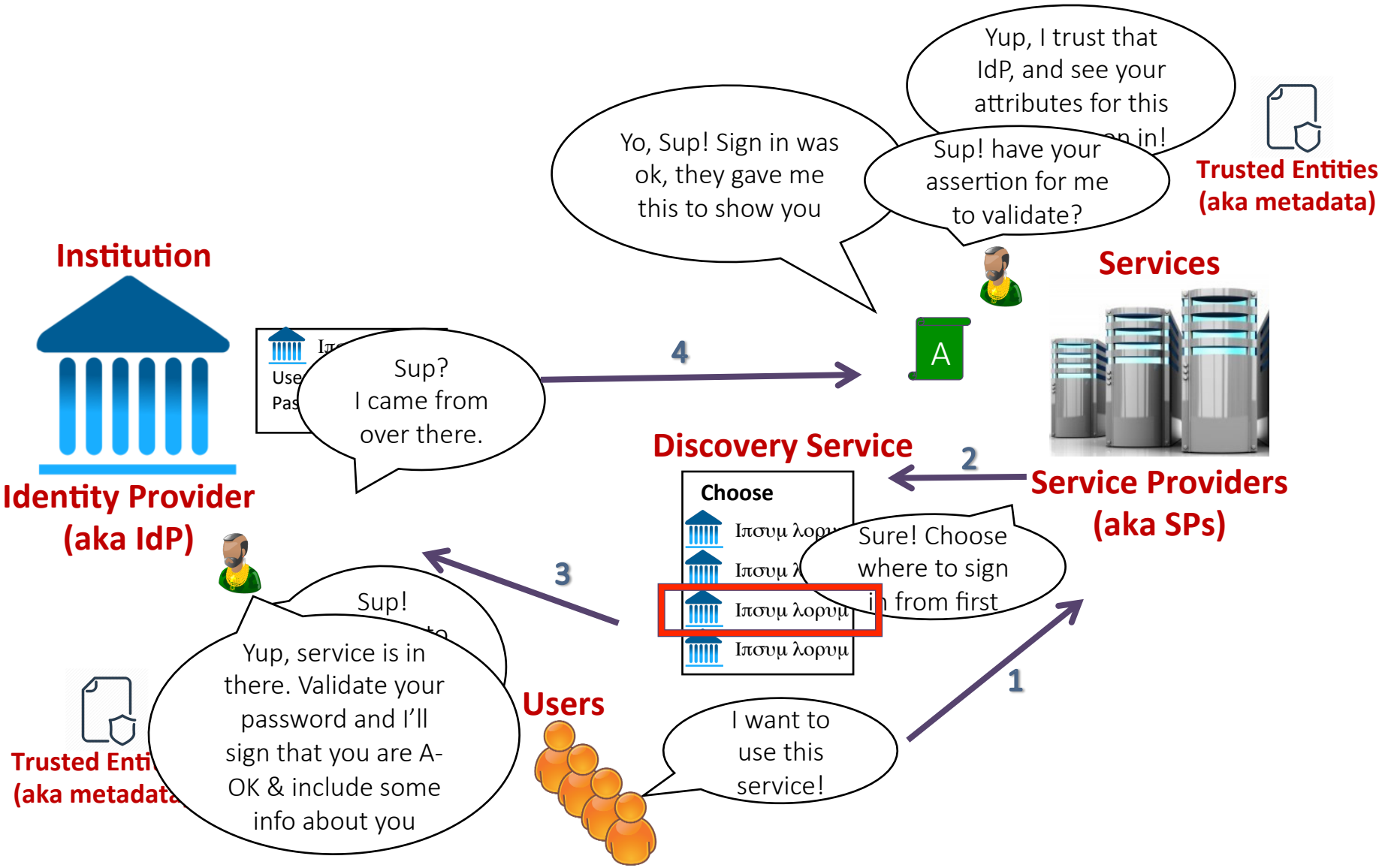
> Test Installation
  - Planning ~ ½ to 1 person day effort
  - Post installation: ~ ¼ to 2 person effort
  - Testing: ~ ½ to 2 person day effort

> Influencing factors:
  - Complexity of customizations (i.e. more than a logo?)
  - Readiness of resources (e.g. vm, firewall settings)
  - Full time and attention – or not
  - Produces portable configuration file
  - Time reduction re-uses portable configuration
  - Can run 'headless' for automated install

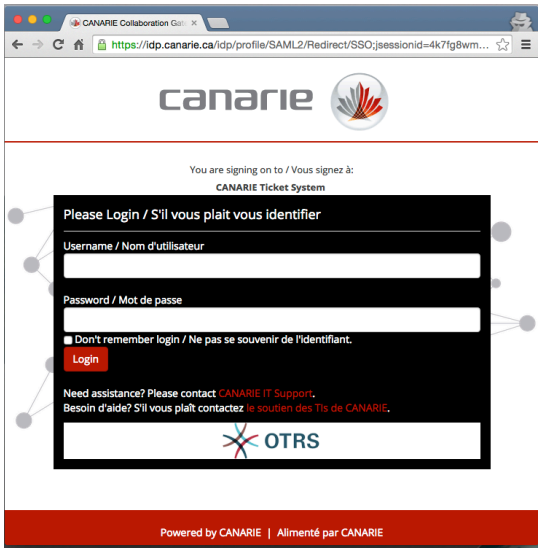
canarie

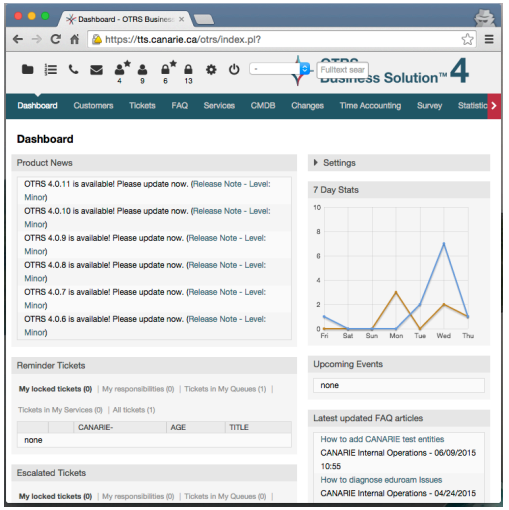
canarie.ca | @canarie_inc

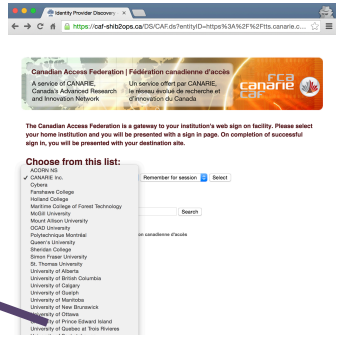
What happens and who's involved?



Demo



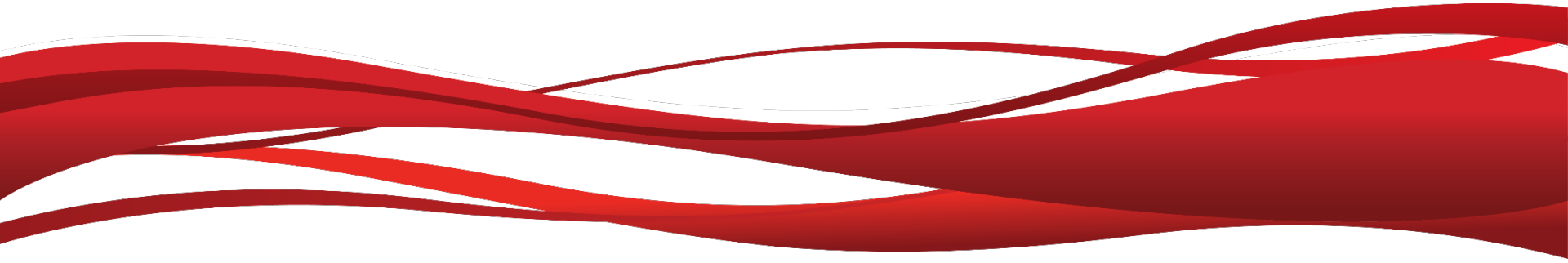




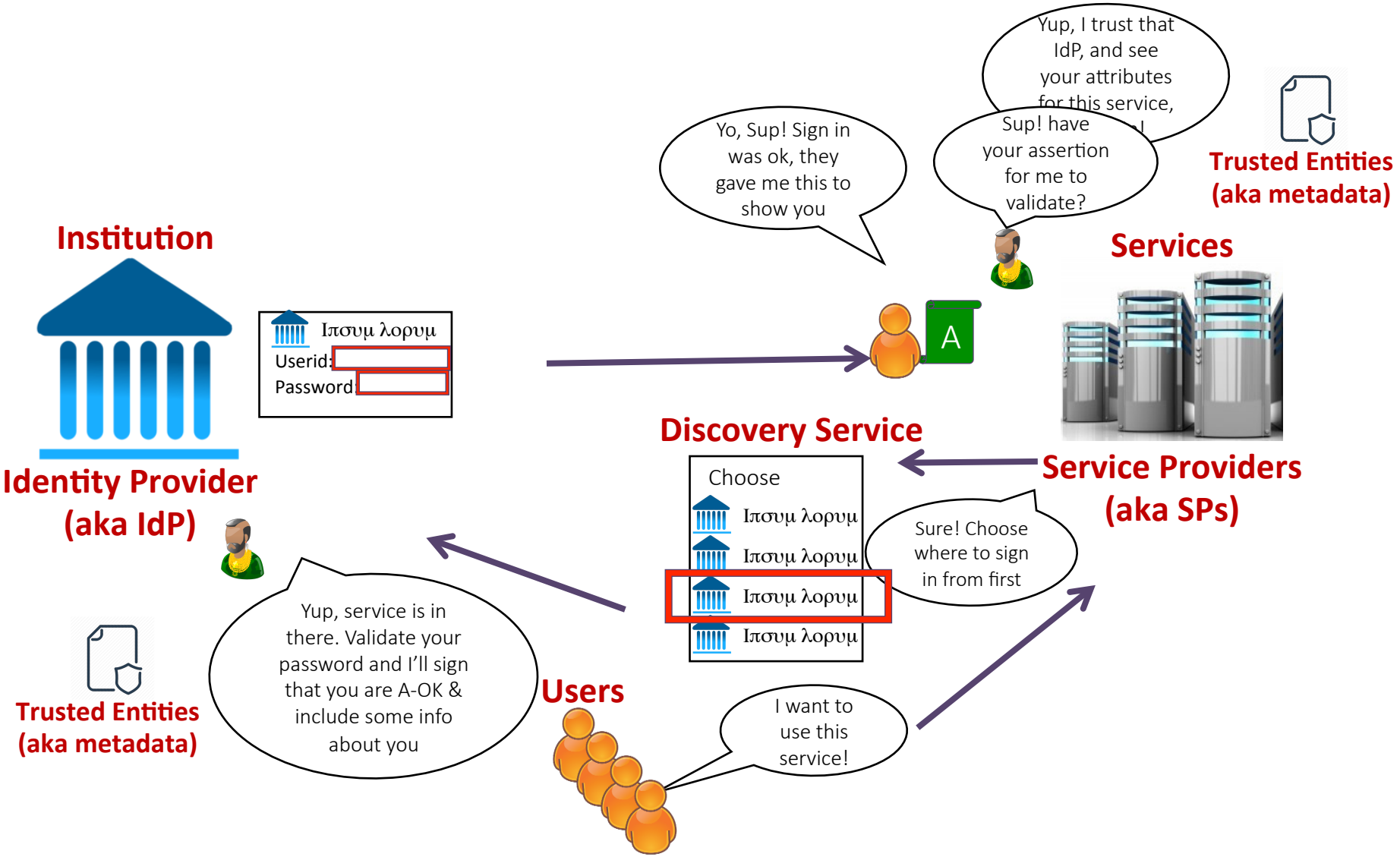
Sure! Choose where to sign in from first

I want to use this service!

How do we know what to trust?



How CAF Scales Federation Trust



How CAF Delivers Federation Trust at Scale

Federation Operator

Builds, Signs and Curates

Trusted Entities (aka metadata)

Trusted Entities (aka metadata)

Services

Service Providers (aka SPs)

Institution

Identity Provider (aka IdP)

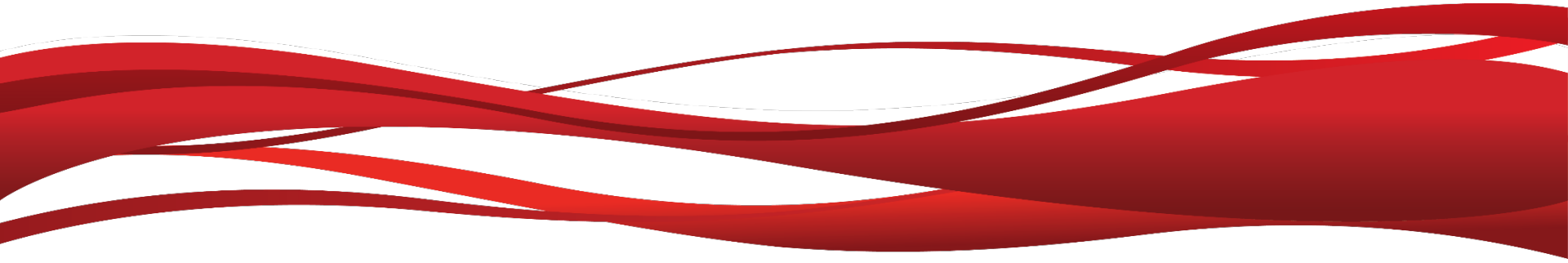
Sites retrieve file hourly
Cached by all participants

Trusted Entities (aka metadata)

Avoids N by M problem:

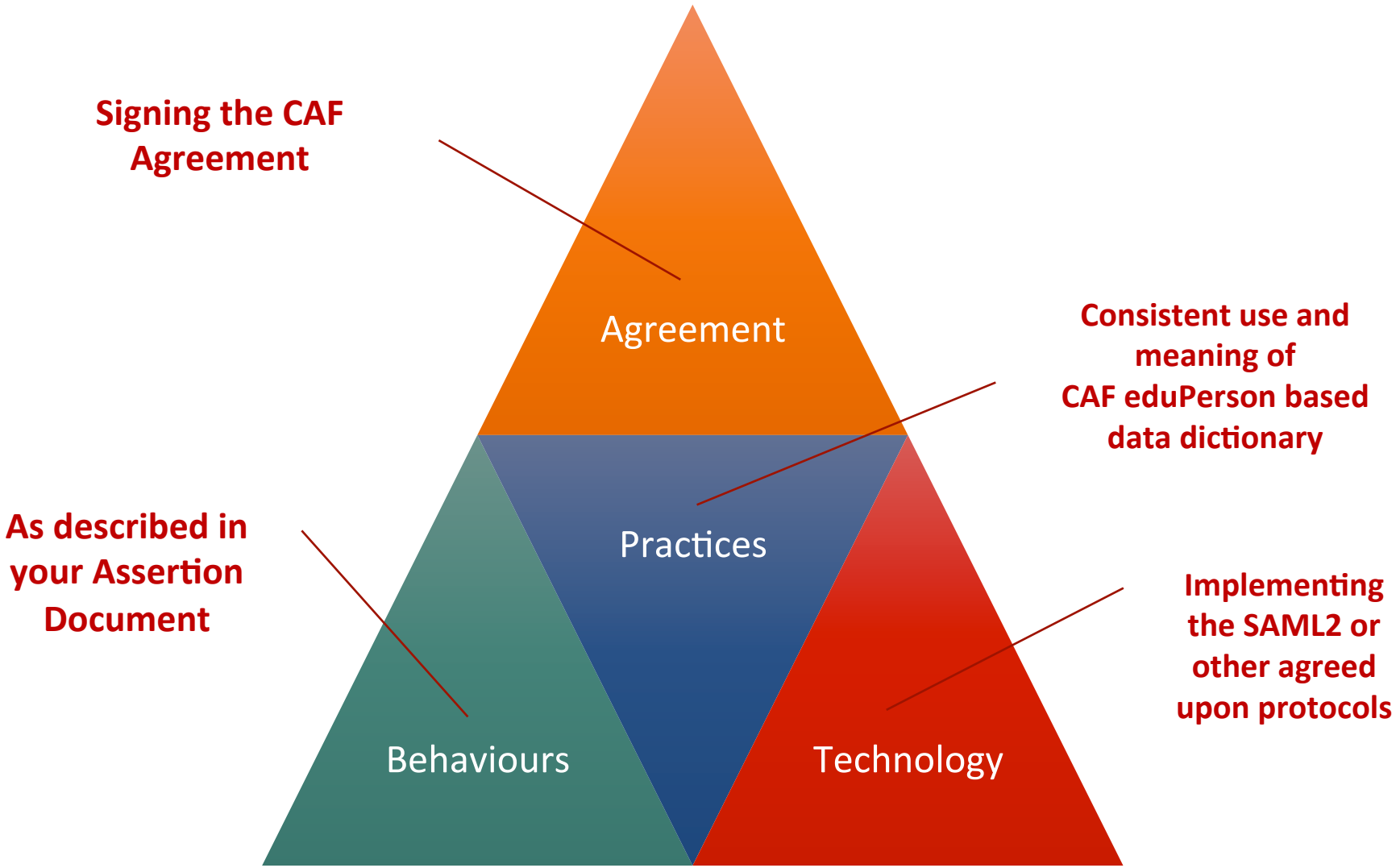
- Metadata trust model scales regardless of number of sites
- Cryptographically signed to ensure veracity

How do we know what to trust?




?RUST

Federation Trust in Concrete Terms



How Do I Use This Info?

> Identify where you are on the spectrum

> Workshop objectives:

- Become more knowledgeable
- Be a solution expert
- Be able to recommend options