RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: IDY-F02

DON'T Use Two-Factor Authentication...

Unless You Need It!

Michael Schwartz

CEO
Gluu, Inc.
@gluufederation

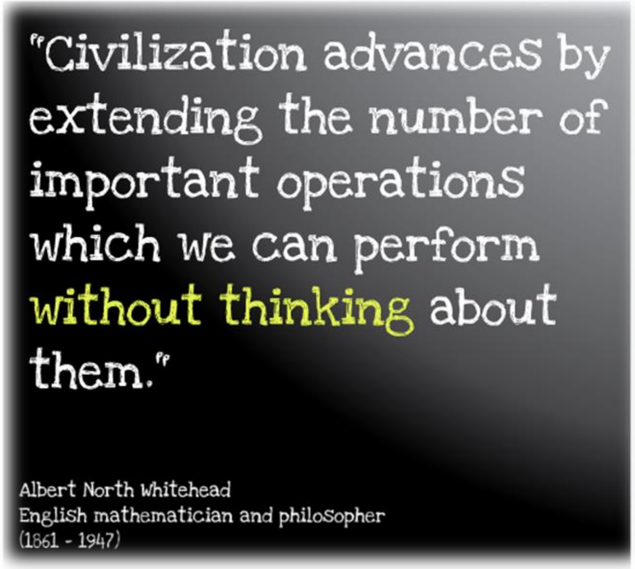
#RSAC

Obama says use two factors…

"…encourage more Americans to move beyond passwords - adding an extra layer of security like a fingerprint or codes sent to your cellphone."

https://nakedsecurity.sophos.com/2016/02/12/obama-says-passwords-arent-strong-enough-urges-use-of-2fa/

Progress = Obliviousness

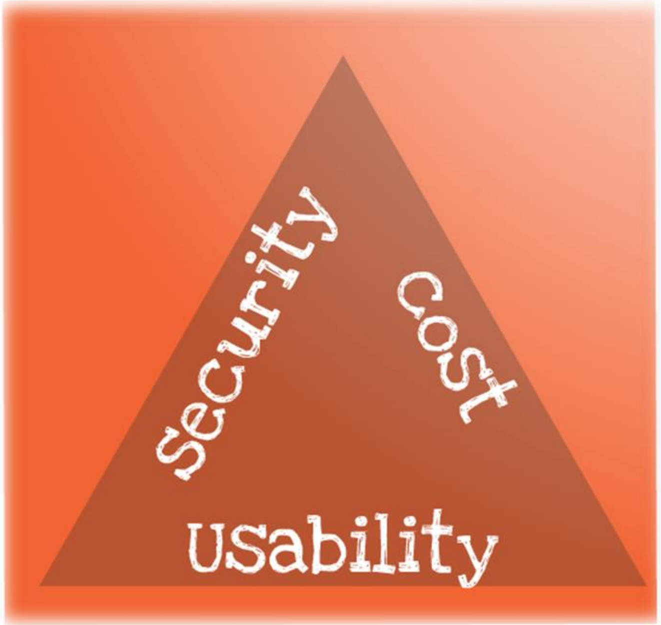


"Civilization advances by extending the number of important operations which we can perform without thinking about them."

Albert North Whitehead
English mathematician and philosopher
(1861 - 1947)

2FA = two-factor authentication

Authentication tradeoffs…



Protect your money!

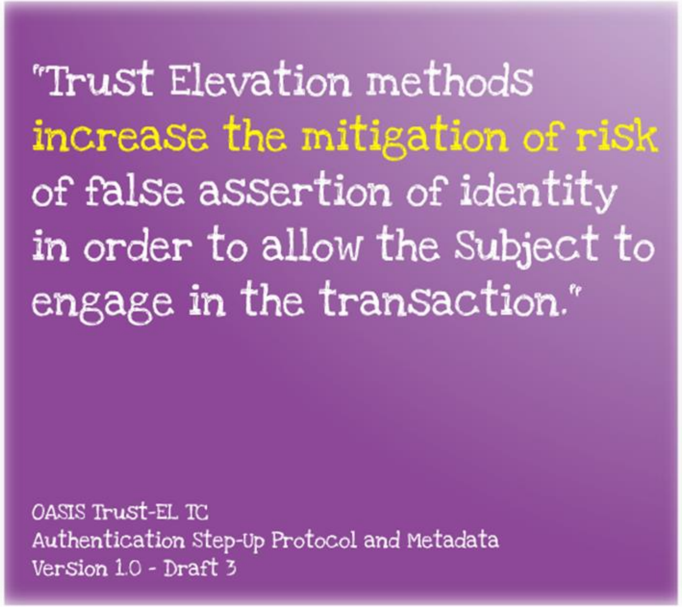
- Issued guidance in 2005 entitled “Authentication in an Internet Banking Environment“

FFIEC

“… the techniques employed should be commensurate with the risks associated with the products and services offered ”

Source: https://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf

What is Trust Elevation?



"Trust Elevation methods **increase the mitigation of risk** of false assertion of identity in order to allow the Subject to engage in the transaction."

OASIS Trust-EL TC
Authentication Step-Up Protocol and Metadata
Version 1.0 - Draft 3

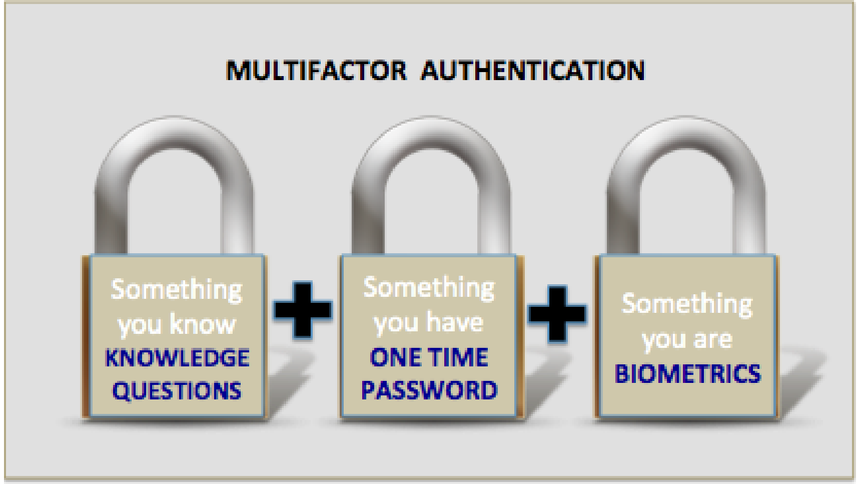
Agenda

- Background on authentication technology: where are we today?
- Deep Dive into OAuth2: what features does it have to support Trust Elevation
- Trust Elevation across domain boundaries

GOAL: Make you aware of some of the challenges we face to enable Trust Elevation

What is Multi-Factor Authentication?

- NIST defines this as two or more of …
  - Something you know
  - Something you have
  - Something you are



Source: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

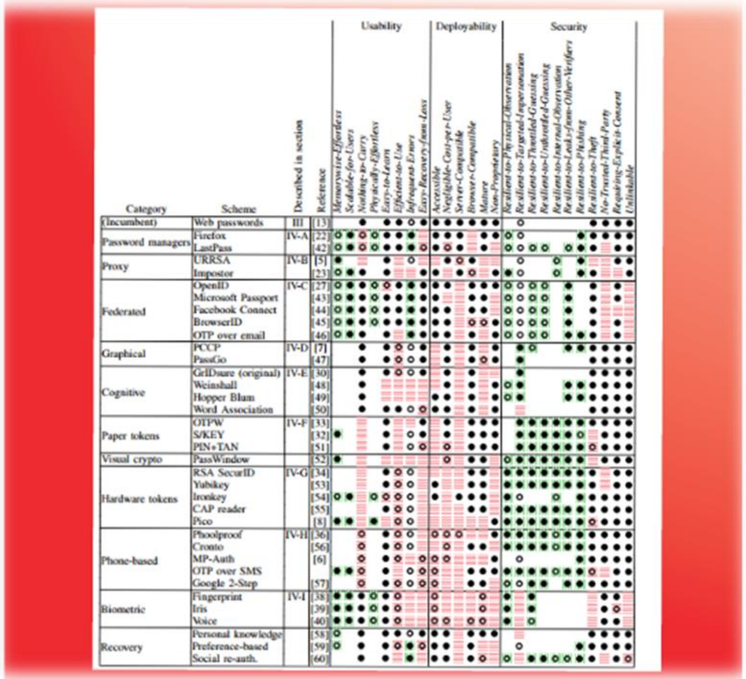
Risk Scores

EARLY WEB FRAUD DETECTION
MID-RISK CUSTOMER
SCORE: 215
HISTORY
REPUTATION
SCRIPT DETECTION
TIMING
COHERENCY
DEVICE
~~CREDIT CARD CYCLYING~~
~~SITE SCRAPING~~
~~ACCOUNT HIJACKING~~
CLICK FRAUD
~~ONLINE PAYMENT FRAUD~~
~~APPSTORE RATING FRAUD~~
SCRIPTED REGISTRATION
BUSINESS LOGIC ABUSE

Contextual Combinations Complicate

Is the IP address a known hacker? Was the device rooted? Is a browser cookie present? Is the device running virus protection? Is the location recognized? When was credential issued? What is the time of the day?

"…every scheme does worse than passwords on deployability"



				Usability								Deployability						Security										
Category	Scheme	Described in section	Reference	Memorywise-Effortless	Scalable-for-Users	Nothing-to-Carry	Physically-Effortless	Easy-to-Learn	Efficient-to-Use	Infrequent-Errors	Easy-Recovery-from-Loss	Accessible	Negligible-Cost-per-User	Server-Compatible	Browser-Compatible	Mature	Non-Proprietary	Resilient-to-Physical-Observation	Resilient-to-Targeted-Impersonation	Resilient-to-Throttled-Guessing	Resilient-to-Unthrottled-Guessing	Resilient-to-Internal-Observation	Resilient-to-Leaks-from-Other-Verifiers	Resilient-to-Phishing	Resilient-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Consent	Unlinkable
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●		●	●	●		●	●	○	○					●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●		●		○	○	○	○		○	●	●		●	●
Proxy	URRSA	IV-B	[5]	●				●		○			●	○	●				○			○		●			●	●
	Impostor		[23]	○	●	●		●			●	●		●	○		●	●	○			○		●	●			●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●		●	●	●	○	○	○	○		●		●		●	
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●			●	●		○	○	○	○		●		●		●	
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●		●	●		○	○	○	○		●		●			
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●		○	○	●	○	○	○	○		●		●		●	
	OTP over email		[46]	○	●	●		●		●	●	●	●		●		●	○	○	○	○		●	●	●		●	
Graphical	PCCP	IV-D	[7]			●		●	○	○	●		●		●		●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●		●		●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●		●		●				●						●	●	●	●
	Weinshall		[48]			●							●		●		●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●						●	●		●		●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●		●		●								●	●	●	●
Paper tokens	OTPW	IV-F	[33]					●			●		●		●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●				●		○	●		●		●	●	●		●	●	●	●	●	○		●	●	●
	PIN+TAN		[51]					●		○	○		○		●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●									○		●	●		○	●	●	●	●	●	●		●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]					●	○	○					●	●		●	●	●	●	●	●	●	●		●	●
	Yubikey		[53]					●	○	○		●			●	●		●	●	●	●	●	●	●	●		●	●
	Ironkey		[54]	○	●		○	○	○	○		●		●	●	●		●	○			○		●	●	●	●	●
	CAP reader		[55]					●	○	○					●	●		●	●	●	●	●	●	●	●	●	●	●
	Pico		[8]	●	●		●		○	○							●	●	●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○		○	○	○			●	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○			○		●	●		●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○		○	○	○				●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●		○	○	○			●	●	●	●	●	●	●	○	●	●	○		●	●
	Google 2-Step		[57]			○		●	○	○	○	○			●	●		○	○	●	●		●	●	●	●	●	●
Biometric	Fingerprint	IV-I	[38]	●	●	●	○	●	○			○				○		●		●						●	●	
	Iris		[39]	●	●	●	○	●	○			○				○		●		●						●	○	
	Voice		[40]	●	●	●	○	●	○			○	○		○	○		●		○						●	●	
Recovery	Personal knowledge		[58]	○		●		●	●	○	●	●	●		●	●	●								●	●	●	●
	Preference-based		[59]	○		●		●	○	●	○	●	●		●				○					●	●	●	●	●
	Social re-auth.		[60]			●		●		●		●	●		●	○		○		●	●	○	○	●	●		●	○

http://research.microsoft.com/pubs/161585/QuestToReplacePasswords.pdf

OAuth2 will make 2FA more “deployable”

No “one-offs”

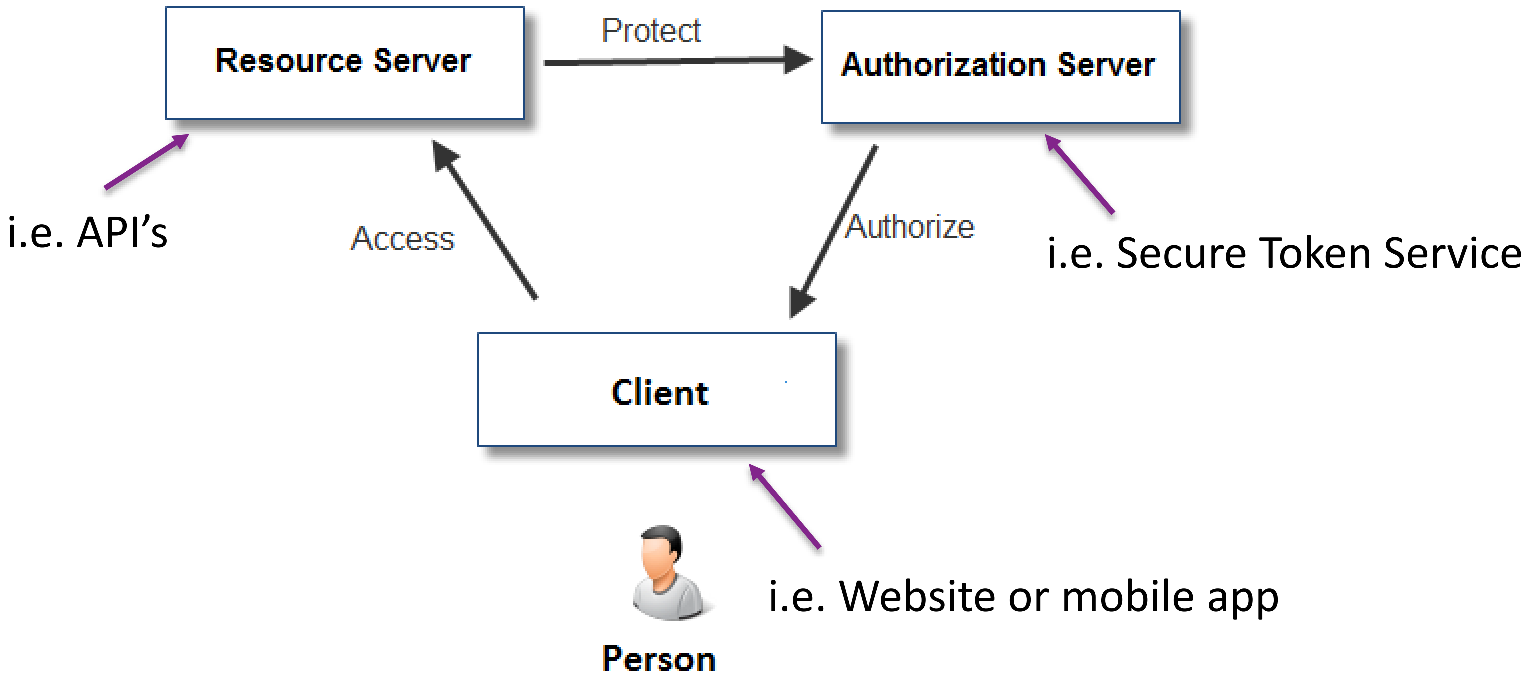
OpenID Connect

UMA

Applications should use Standard API’s for authentication and Trust Elevation!

Good Intro to OAuth2:
http://nordicapis.com/api-security-oauth-openid-connect-depth/

Enter OAuth2



Resource Server

Protect

Authorization Server

i.e. API’s

Access

Authorize

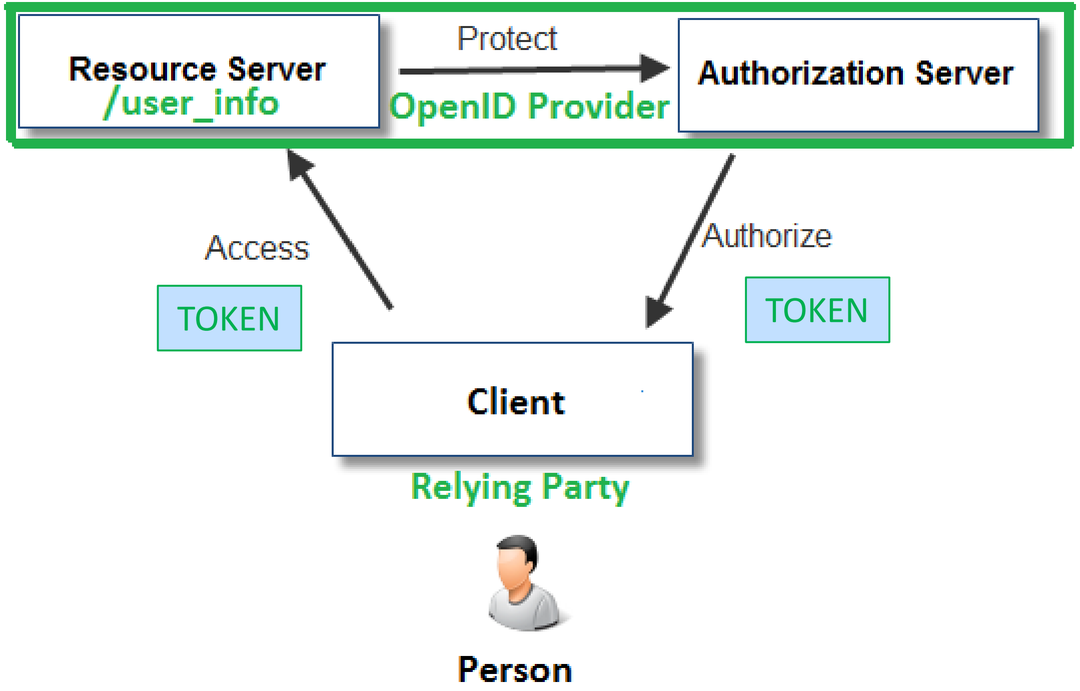
i.e. Secure Token Service

Client

i.e. Website or mobile app

Person

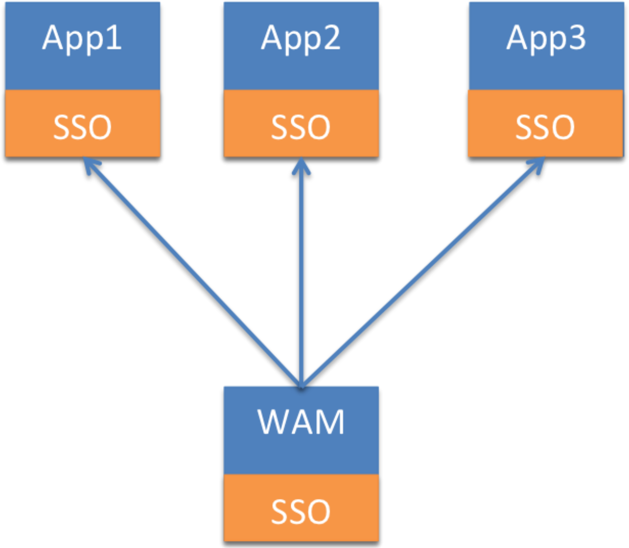
OpenID Connect



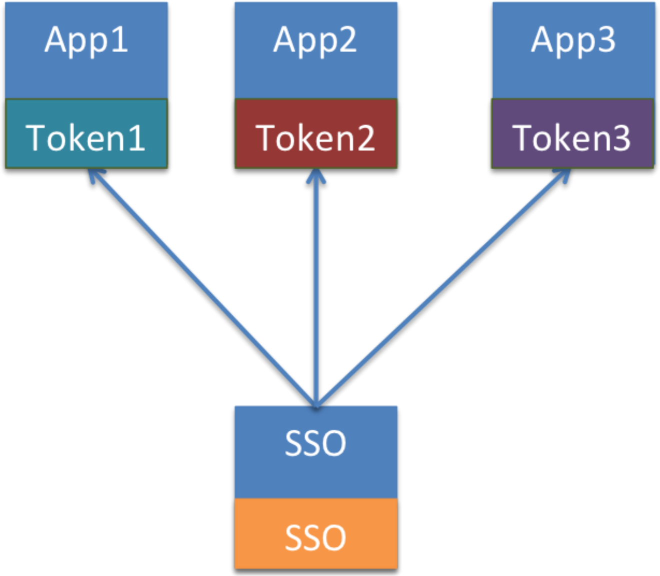
Resource Server = **user_info** API

To call this API, you need an **Access Token**

Importance of Audience



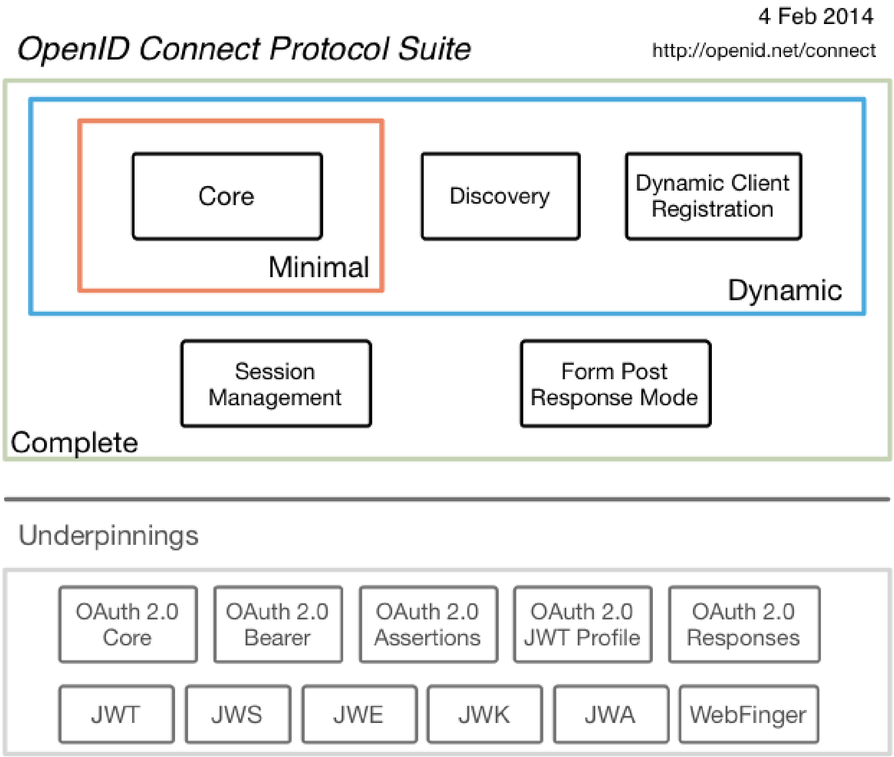
BEFORE



AFTER

https://hanszandbelt.wordpress.com/2015/12/14/the-importance-of-audience-in-web-sso/

OpenID Connect: Client Registration, Discovery too!



4 Feb 2014

OpenID Connect Protocol Suite

http://openid.net/connect

Core

Minimal

Discovery

Dynamic Client Registration

Dynamic

Session Management

Form Post Response Mode

Complete

Underpinnings

OAuth 2.0 Core

OAuth 2.0 Bearer

OAuth 2.0 Assertions

OAuth 2.0 JWT Profile

OAuth 2.0 Responses

JWT

JWS

JWE

JWK

JWA

WebFinger

http://openid.net/connect

Overview of Authorization Code Flow

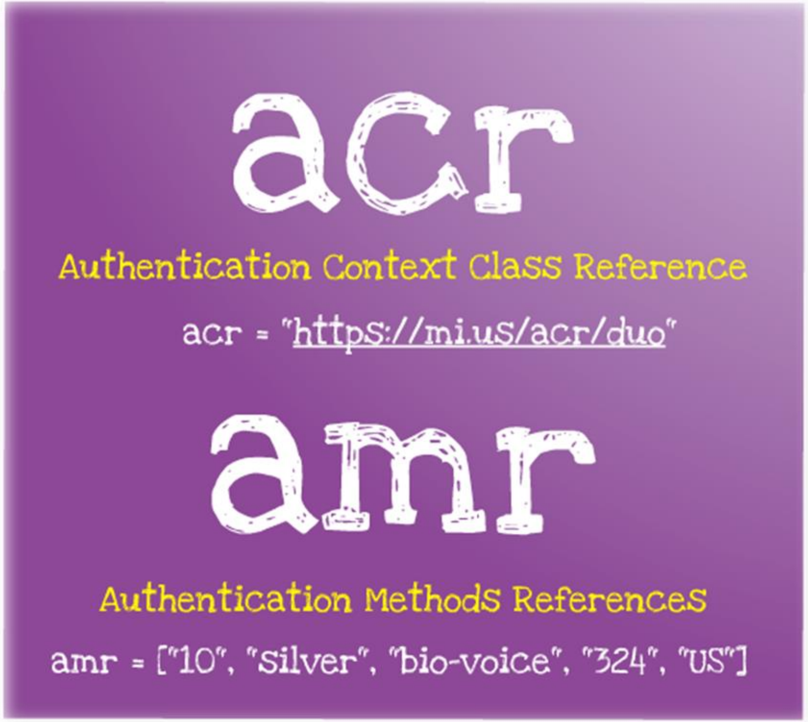
- Relying Party (RP) redirects person to OpenID Provider (OP) for authorization
  - Authentication happens only once!
- OP returns **code** to RP
- RP uses **code** to get **tokens** from OP
- RP uses **access token** to obtain **user claims** from **/user_info** API:
  {“given_name”: “Mike”,
  “family_name”: “Schwartz”}

OpenID Connect id_token

```
{
 "iss": "https://server.example.com",
 “sub": "248289761001",
 "aud": "3214244",
 "iat": 1311195570,
 "exp": 1311281970,
 “auth_time”: 131195001,
 “acr”: http://example.com/basic_bio”
 “amr”: [‘eye’, ‘pwd’, ‘12’]
}
```

Information about authentication event

ACR and AMR



acr

Authentication Context Class Reference

acr = "https://mi.us/acr/duo"

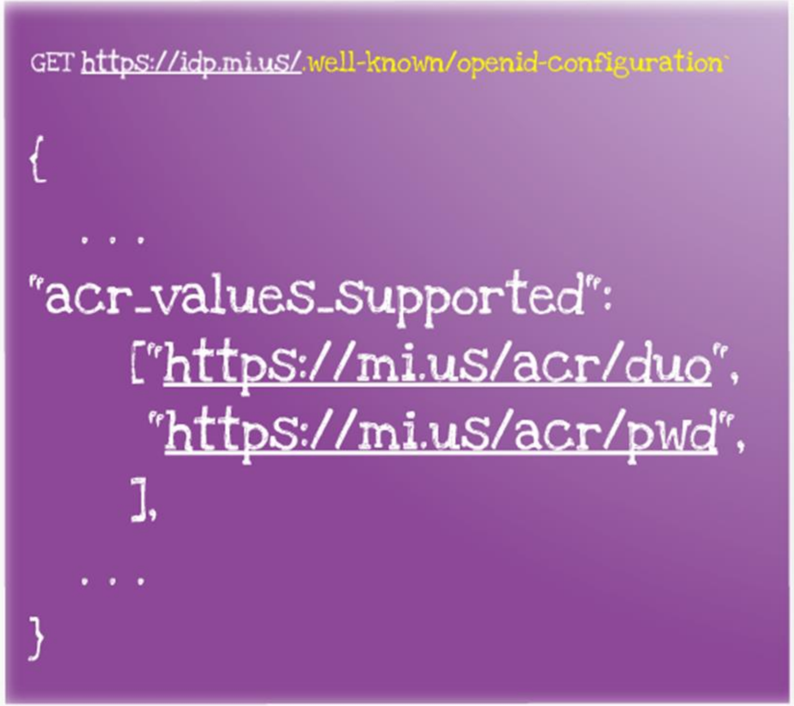
amr

Authentication Methods References

amr = ["10", "silver", "bio-voice", "324", "US"]

How does the app know what kind of authentication happened?

OpenID Provider Discovery

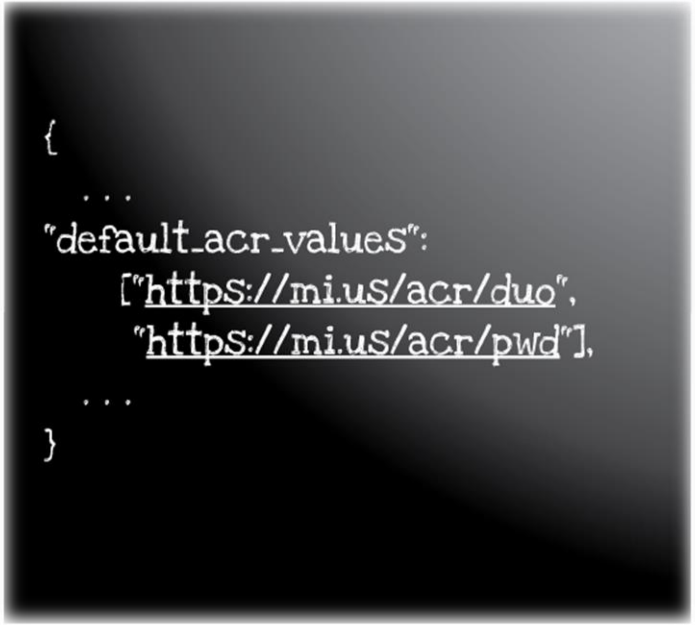


```
GET https://idp.mi.us/.well-known/openid-configuration

{
    . . .
"acr_values_supported":
      ["https://mi.us/acr/duo",
       "https://mi.us/acr/pwd",
      ],
    . . .
}
```

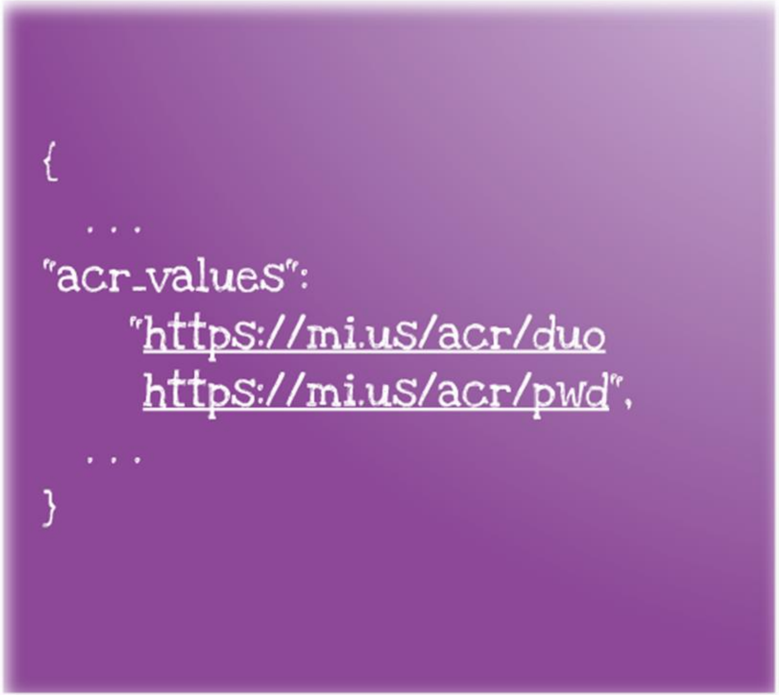
GET host + /.well-known/openid-configuration

OpenID Dynamic Client Registration



```
{
   . . .
"default_acr_values":
      ["https://mi.us/acr/duo",
       "https://mi.us/acr/pwd"],
   . . .
}
```

Authentication Request



```
{
  ...
"acr_values":
    "https://mi.us/acr/duo
     https://mi.us/acr/pwd",
  ...
}
```

In the request, **acr_values** is actually a space delimited string…

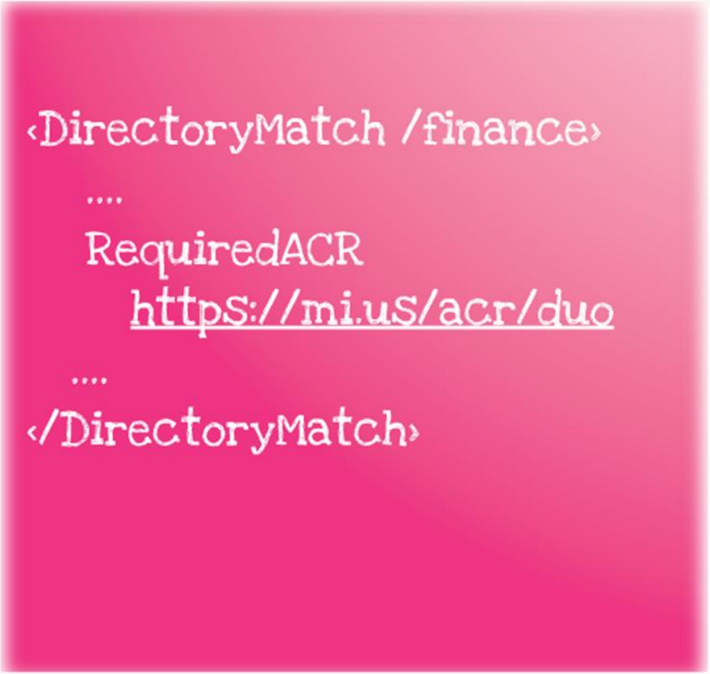
id_token

```
{
 "iss": "https://server.example.com",
 “sub": "248289761001",
 "aud": "3214244",
 "iat": 1311195570,
 "exp": 1311281970,
 “auth_time”: 131195001,
 “acr”: http://example.com/basic_bio”
 “amr”: [‘eye’, ‘pwd’, ‘12’]
}
```

Returned **id_token** confirms **acr** and **amr** values

App Policy

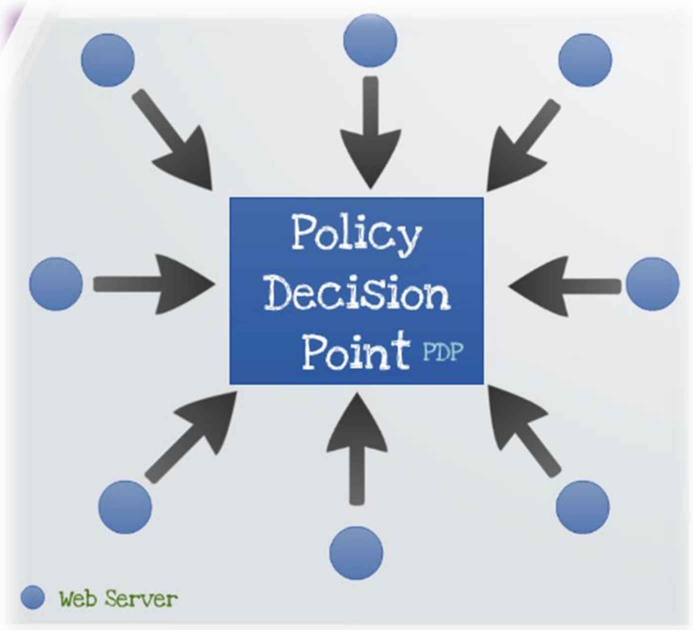
GET https://example.com/finance



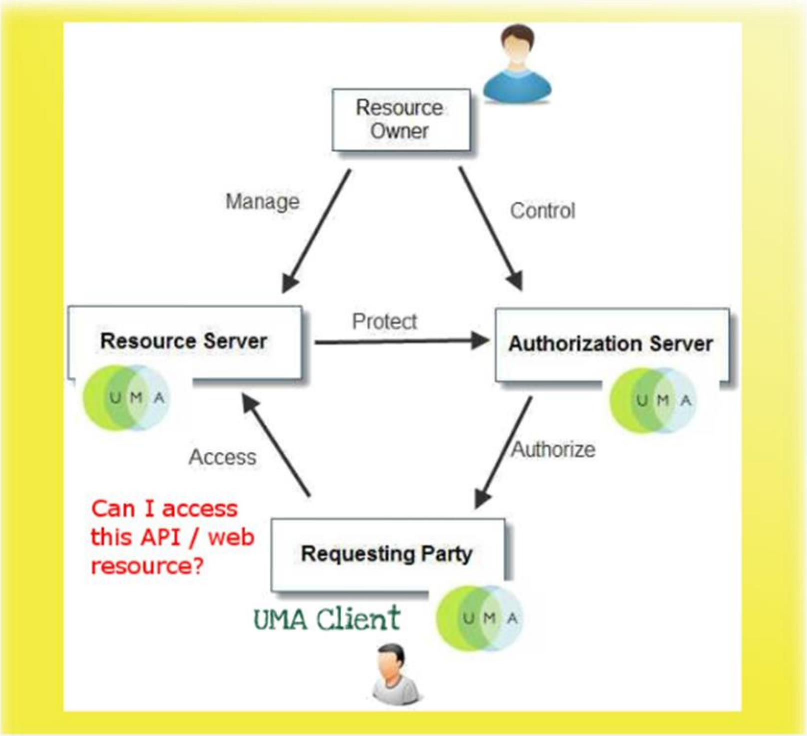
```
<DirectoryMatch /finance>
    ....
    RequiredACR
        https://mi.us/acr/duo
   ....
</DirectoryMatch>
```

Just an example…
using OpenID Connect alone,
you could require a certain
type of authentication

Best Practice:
Centralize Policy Management

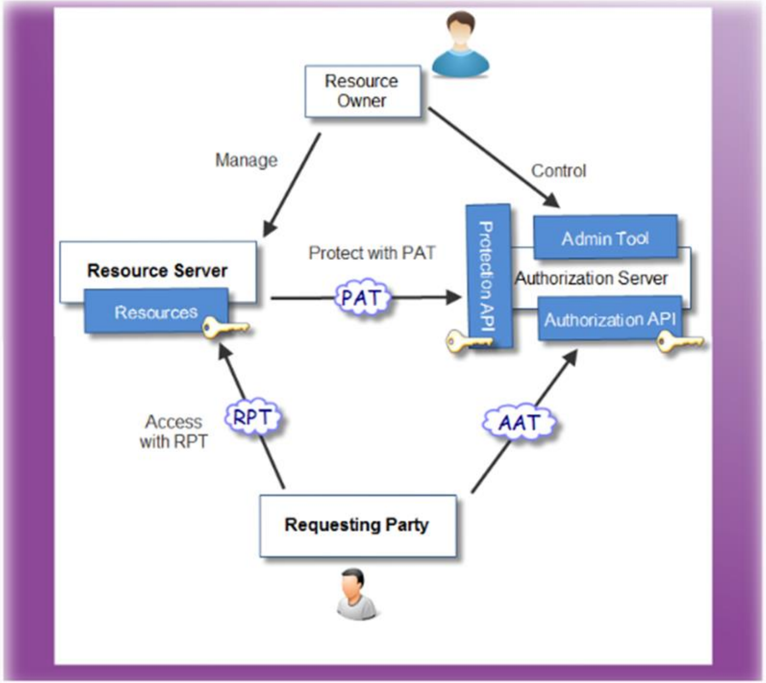


UMA



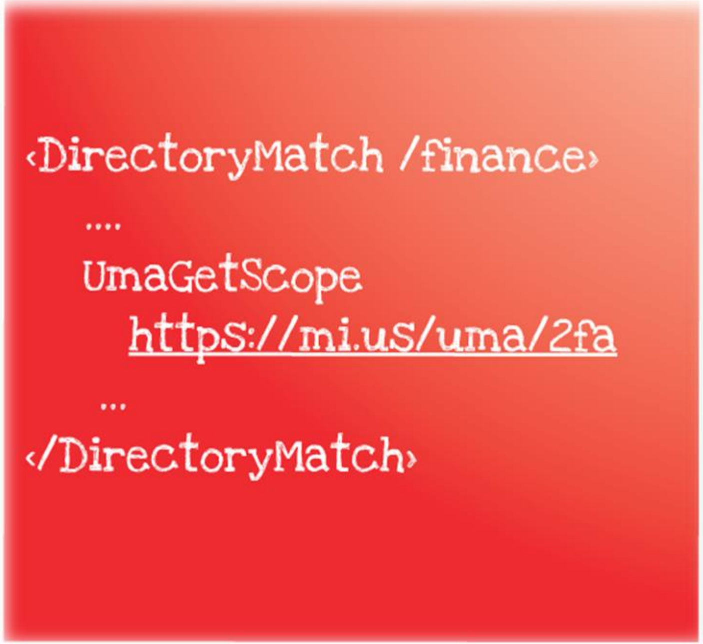
Protect **any** API:
require an
RPT Token

UMA In 60 seconds



- Client Calls API without RPT Token
- RS obtains Permission Ticket from AS and returns it to Client
- Client presents ticket to AS
- AS evaluates polices. If ok, issues RPT token (bearer)
- Client calls API with RPT Token
- RS introspects Token: if ok, returns content

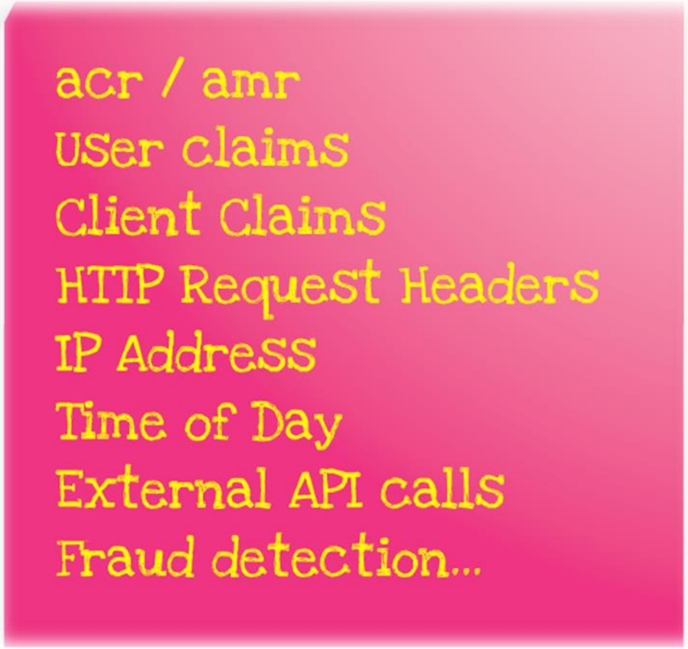
Subtle difference…
Scope references policy



```
<DirectoryMatch /finance>
    ....
    UmaGetScope
      https://mi.us/uma/2fa
    ...
</DirectoryMatch>
```

Scope based access:
Level of abstraction that enables the central policy decision point to decide which **acr** is required

What kind of policies can you make?



acr / amr

User claims

Client Claims

HTTP Request Headers

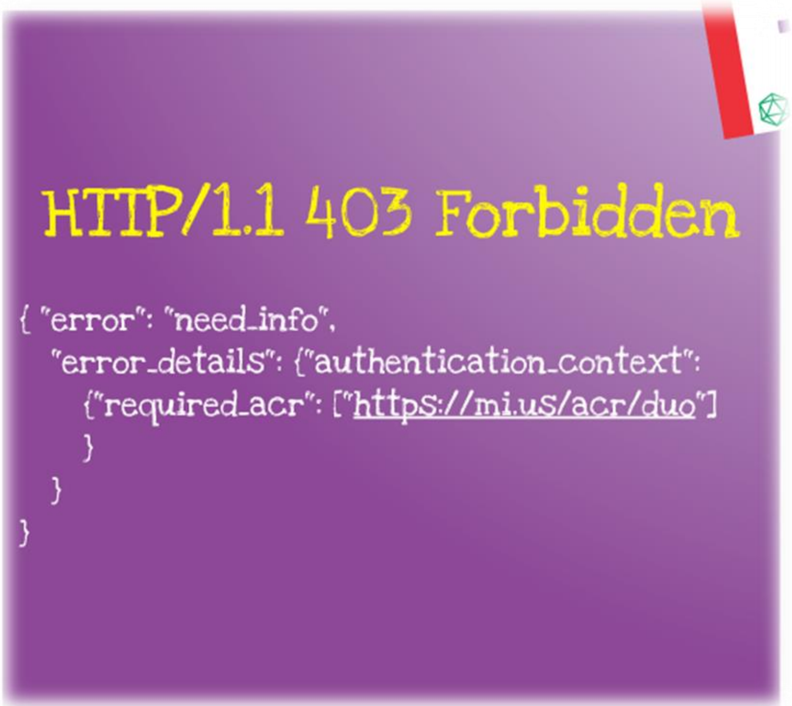
IP Address

Time of Day

External API calls

Fraud detection...

Elevating Trust using UMA

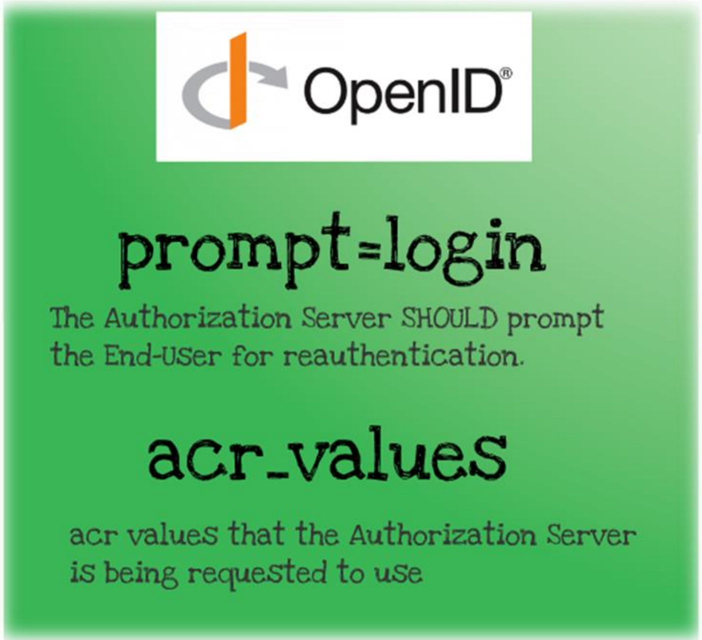


HTTP/1.1 403 Forbidden

```
{ "error": "need_info",
  "error_details": {"authentication_context":
    {"required_acr": ["https://mi.us/acr/duo"]
    }
  }
}
```

You are Forbidden because you need acr…

Re-Authenticate!



OpenID®

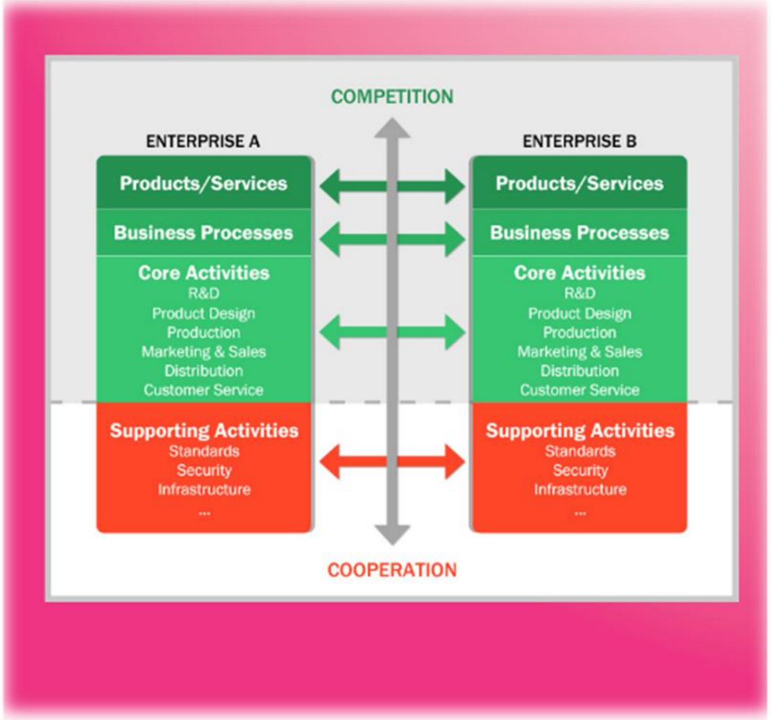
prompt=login

The Authorization Server SHOULD prompt the End-User for reauthentication.

acr_values

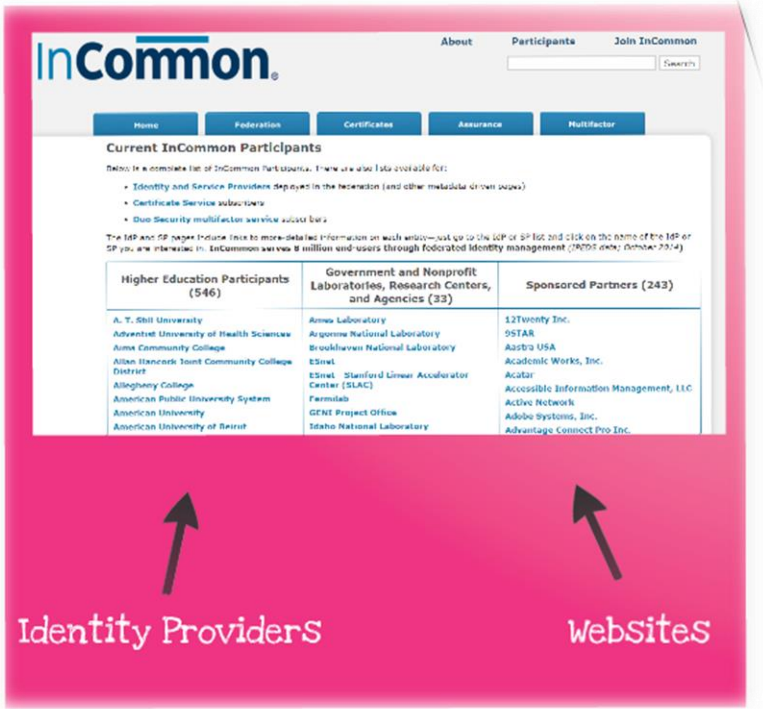
acr values that the Authorization Server is being requested to use

Part III: Intedomain trust elevation



Infrastructure and security is not (usually) basis for competition between firms in the same industry.

SAML Federations



Current InCommon Participants

Below is a complete list of InCommon Participants. There are also lists available for:

- Identity and Service Providers deployed in the federation (and other metadata driven pages)
- Certificate Service subscribers
- Duo Security multifactor service subscribers

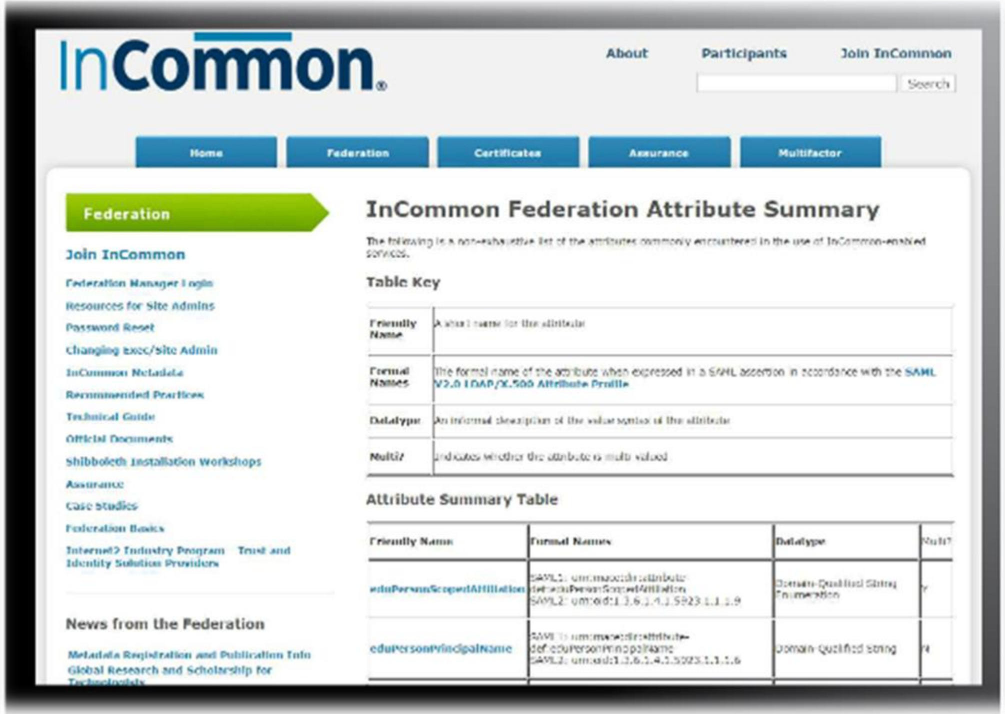
The IdP and SP pages include links to more-detailed information on each entity—just go to the IdP or SP list and click on the name of the IdP or SP you are interested in. InCommon serves 8 million end-users through federated identity management (IPEDS data; October 2014)

Higher Education Participants (546)	Government and Nonprofit Laboratories, Research Centers, and Agencies (33)	Sponsored Partners (243)
A. T. Still University	Ames Laboratory	12Twenty Inc.
Adventist University of Health Sciences	Argonne National Laboratory	9STAR
Aims Community College	Brookhaven National Laboratory	Aastra USA
Allan Hancock Joint Community College District	ESnet	Academic Works, Inc.
Allegheny College	ESnet - Stanford Linear Accelerator Center (SLAC)	Acatar
American Public University System	Fermilab	Accessible Information Management, LLC
American University	GENI Project Office	Active Network
American University of Beirut	Idaho National Laboratory	Adobe Systems, Inc.
		Advantage Connect Pro Inc.

Normalize legal/technical

Many SAML Federations publish user schema.

http://www.incommon.org/federation/attributesummary.html



InCommon Federation Attribute Summary

The following is a non-exhaustive list of the attributes commonly encountered in the use of InCommon-enabled services.

Table Key

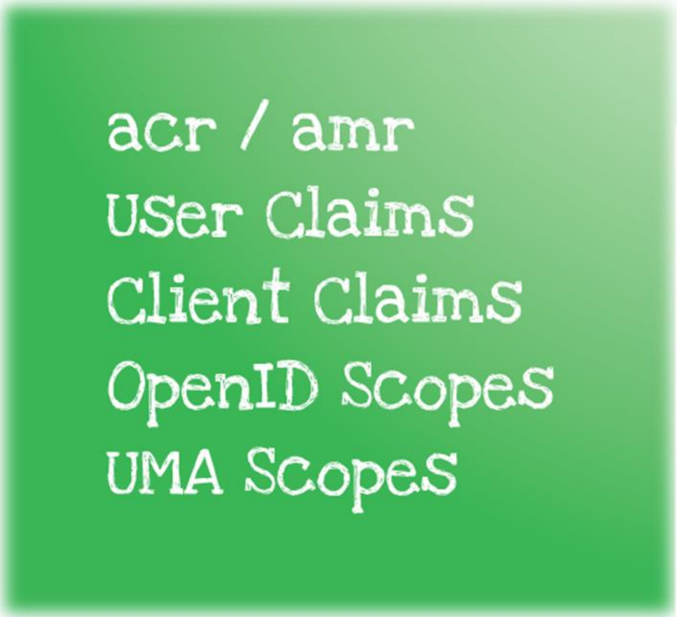
Friendly Name	A short name for the attribute
Formal Names	The formal name of the attribute when expressed in a SAML assertion in accordance with the SAML V2.0 LDAP/X.500 Attribute Profile
Datatype	An informal description of the value syntax of the attribute
Multi?	Indicates whether the attribute is multi valued

Attribute Summary Table

Friendly Name	Formal Names	Datatype	Multi?
eduPersonScopedAffiliation	SAML1: urn:mace:dir:attribute-def:eduPersonScopedAffiliation SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.9	Domain-Qualified String Enumeration	Y
eduPersonPrincipalName	SAML1: urn:mace:dir:attribute-def:eduPersonPrincipalName SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.6	Domain-Qualified String	N

gluu

OAuth2 schema: not just user claims…



acr / amr

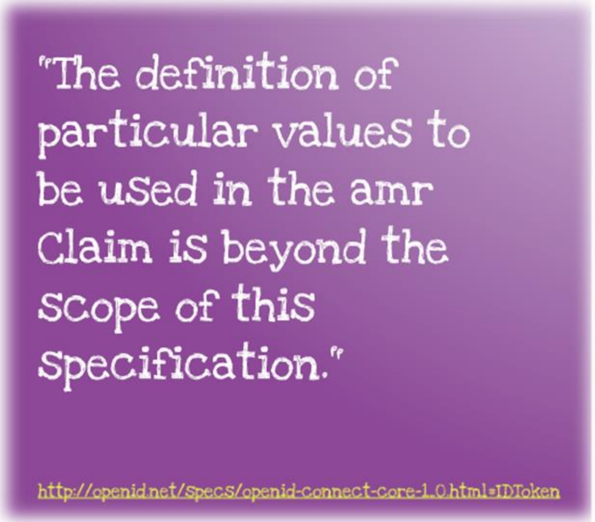
User Claims

Client Claims

OpenID Scopes

UMA Scopes

Collaboration on ACR / AMR values



"The definition of particular values to be used in the amr Claim is beyond the scope of this specification."

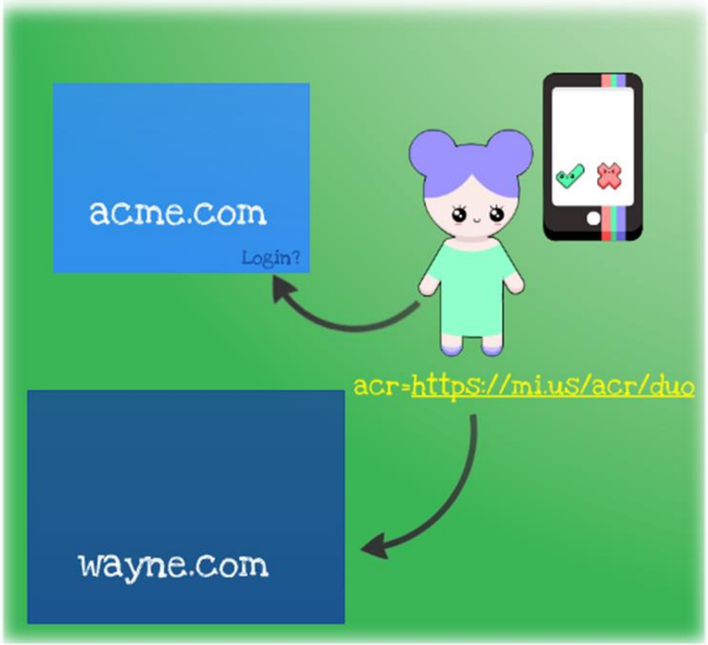
http://openid.net/specs/openid-connect-core-1.0.html#IDToken

So what values should we use for amr and acr?

This IETF draft defines some AMR's… but its inadequate

https://tools.ietf.org/html/draft-jones-oauth-amr-values-05

ACR alignment



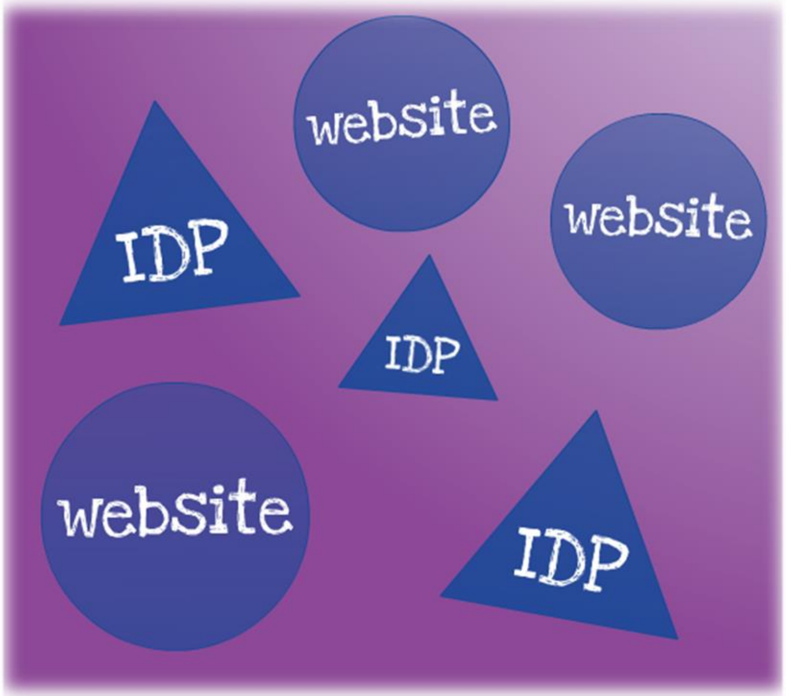
Domains need to collaborate on the values for acr's and amr's

OTTO – Kantara Initiative Work Group

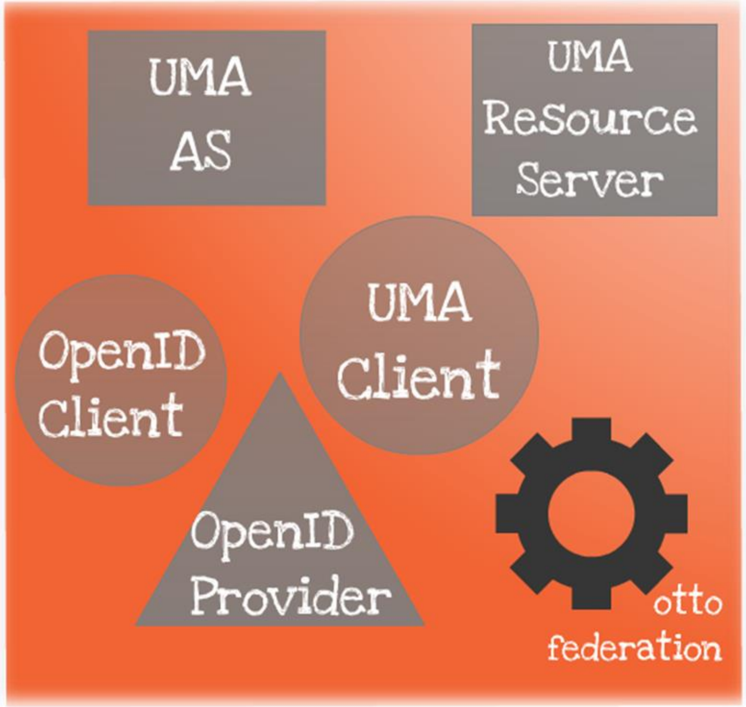
Open Trust Taxonomy for OAuth2

http://kantarainitiative.org/confluence/display/OTTO/Home

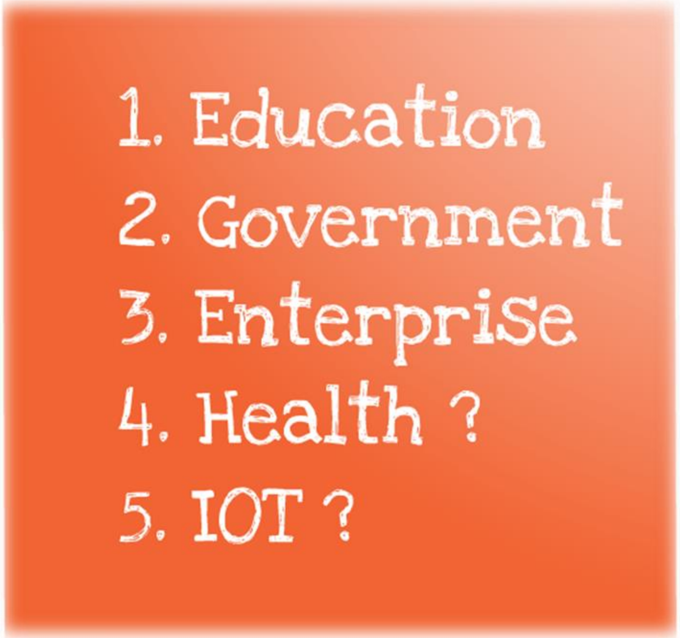
SAML federations



OAuth2 has new entities and new jargon



Where do we need federations



1. Education
2. Government
3. Enterprise
4. Health ?
5. IOT ?

Summary

- We don’t lack ways to identify people, but we lack agreement on the relative strength of these mechanisms.
- OAuth2 enables centralized risk based trust elevation, driving down the cost of deployment—the main impediment to 2FA adoption.
- To enable trust elevation across domains, federations are needed.

Action items

- Don’t limit your planning to two-factor authentication. Make a plan for trust elevation!
- Start architecting your applications to leverage central policy decision point—not for all fine grained authorization, but for key security escalations.
- If you work in an ecosystem, consider collaborating (even with your competitors) to drive down the cost of security.

Thank You!
@gluufederation