

Future Directions in FIM

David W Chadwick

19 Feb 2014

© 2010-14 TrueTrust Ltd

1

Contents

- Attribute Aggregation
- VOMS
- FIM and CLOUDS
- ABFAB
- Inter-Federations

19 Feb 2014

© 2010-14 TrueTrust Ltd

2

Attribute Aggregation

- Current FIMs do not match use of plastic cards
- We have multiple cards in our wallet and may need to present several of them in a single transaction
 - e.g. Credit Card and Rail Card; Hotel Loyalty Card and Frequent Flyer Card
- Along with self asserted data
- The identity management models today assume that in *any given transaction* the user has one **Identity Provider** (IdP) that will provide **ALL** his/her attributes to the Service Provider (SP)
 - E.g. in CardSpace the user can only select a single card, in SAML/Liberty/Shibboleth the user is redirected to a single IDP to login which provides all his/her attributes
- Some are also open to phishing attacks, since the SP redirects the user's browser to his IdP



19 Feb 2014

© 2010-14 TrueTrust Ltd

3

Proposed IDM Solution

- SPs should **inform users** which attributes they need or desire at the time authorisation is needed, along with the **assurance level**, and should be able to **alter this mid-session**.
- A user should be able to combine the attributes he has from **multiple providers** (IdPs/ Attribute Authorities) into a single session with the current service provider, along with **self asserted attributes**, in order to gain a rich quality of service.
 - E.g. book a hotel room online and present your credit card, hotel loyalty card and frequent flyer card in order to pay, get a free room upgrade and acquire points with your airline,
- User should have **complete control, visibility and constant** over attribute release, and otherwise be privacy protected
- User should only have to **authenticate once** in order to do this
- System should be **resilient to phishing attacks**

19 Feb 2014

© 2010-14 TrueTrust Ltd

4

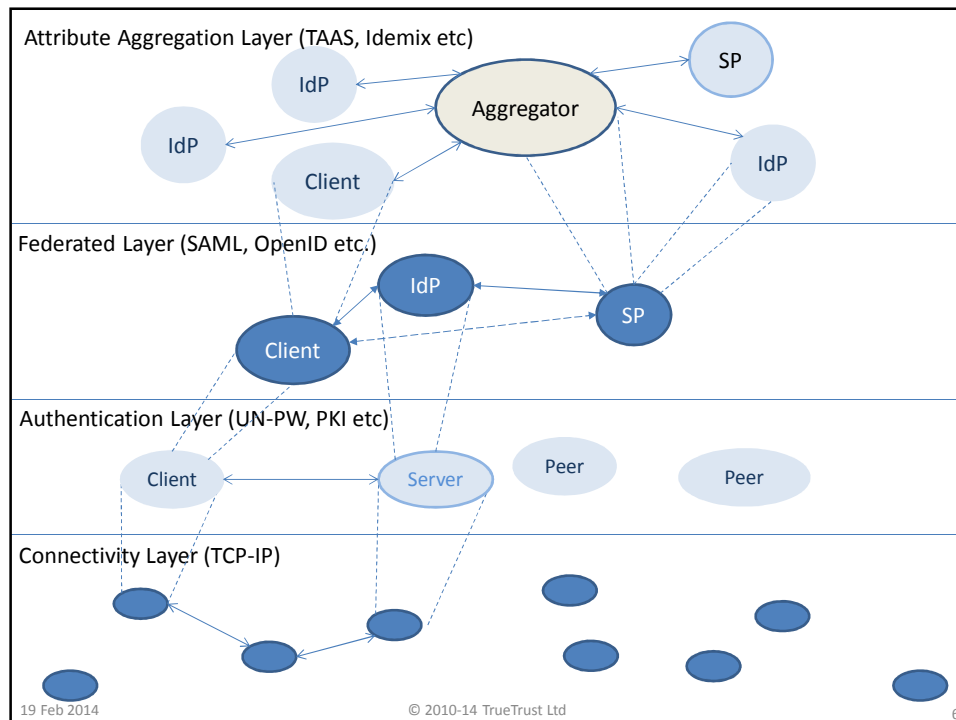
Our Proposal

- To add an attribute authorisation and aggregation layer above the existing federation layer
- Purpose: to provide user attribute aggregation, selection and consent at multiple points during a session with a SP, as the user accesses different protected resource requiring different permissions (attributes and LoAs)

19 Feb 2014

© 2010-14 TrueTrust Ltd

5



Technically Speaking

- The service provider should receive digitally signed attribute assertions from multiple attribute authorities which
 - All belong to the same end user
 - Only release the attributes the user consents to release
 - Give assurance that the person at the other end of the Internet is this end user (and is not a dog)
- Without requiring the user to have to login to each of the attribute authorities
- We propose a **Trusted Attribute Aggregation Service (TAAS)** for this, which is under the control of the user

19 Feb 2014




© 2010-14 TrueTrust Ltd

7

Users are shown which attributes they have to provide

The screenshot shows a web browser window with the URL <https://issrg-beta.cs.kent.ac.uk/taas/borough2/authenticate.php>. The page title is "Borough City Council Online". A breadcrumb trail reads "You Are Here: >> Home >> Parking >> Buy Parking Permit". A message states: "Before proceeding with your purchase we require you to login with a security level of 2 [?] and provide all of the following information".

The required attributes are listed as follows:

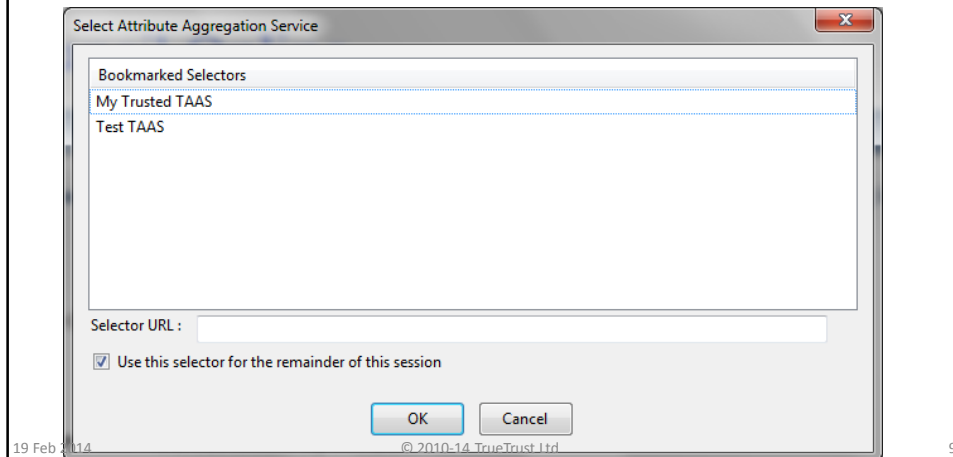
-  Proof of **Car Ownership** issued by the DVLA
-  Proof of **Name and Address** issued by the DWP
-  A **Credit Card** issued by **Visa, Mastercard or American Express**

At the bottom right, there is a blue circular icon with a folder and the text "TAAS". A red arrow points to this icon with the text "User clicks on TAAS icon". Below the icon is a "Get Information" button.

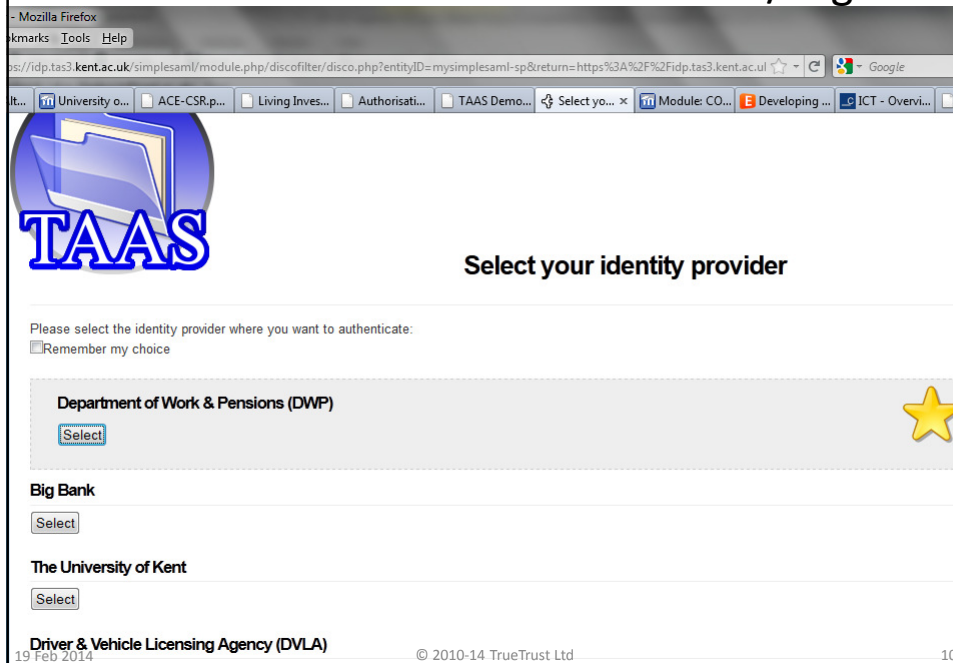
19 Feb 2014 © 2010-14 TrueTrust Ltd 8

User may be asked to select his/her aggregation service

- Users can click on a bookmarked URL (e.g. stored on their own PC)
- Or enter a new URL (e.g. if in Internet café)
- Or SP may ask or be preconfigured with its trusted aggregation service



TAAS now asks user to Authenticate/Login



TAAS filters user's available attribute types against SP's policy

Link Account | Manage my Accounts | Manage my Personal Details | Manage Saved Requests

TAAS

Please choose which of the following you want to use for borough-council2.gov

Cancel

Credit Card ***Required*** Choose

Car Registration ***Required*** Choose

Name ***Required*** Choose

Address ***Required*** Choose

Don't bother me again

Save and Submit Submit

19 Feb 2014 © 2010-14 TrueTrust Ltd 11

Allowing user to select which values he/she wants to use

Link Account | Manage my Accounts | Manage my Personal Details | Manage Saved Requests

TAAS

Please choose which of the following you want to use for borough-council.gov

Cancel

Credit Card ***Required*** Choose

CarRegistration issued by dvia.gov (X.509) ***Required*** Change

Name issued by dwp.gov

Address issued by dwp.gov

Don't bother me again

Save and Submit Submit

Please choose your preferred Credit Card

VisaCard issued by bigbank.com

MasterCard issued by bigbank.com

Submit

19 Feb 2014 © 2010-14 TrueTrust Ltd 11

After completing selection, user submits to SP

Please choose which of the following you want to use for borough-council.gov

Cancel

VisaCard issued by bigbank.com (SomeRandom/Visa) *Required* Change	CarRegistration issued by dvla.gov (X.500 DSA) *Required* Change	Name issued by dwp.gov (David W Chadwick) *Required* Change	Address issued by dwp.gov (1 Some Street...) *Required* Change
--	--	---	--

Don't bother me again

Save and Submit Submit

If user selects this, the saved selection will always be used in future without showing this screen to the user again

User can choose to save selection for next time or submit without saving

19 Feb 2014 © 2010-14 TrueTrust Ltd 13

SP confirms to the user all the actual aggregated attribute values it received from the IdPs

Borough City Council Online

You Are Here: >> Home >> Parking >> Payment Confirmation

Payment Confirmation

A summary of your order is displayed below, please verify that your details are correct before submitting your order.

Name:	David W Chadwick
Address:	1 Some Street Some Area Borough BR68LU
Item:	Limited Parking Permit
Car Reg:	X.500 DSA
Price:	£23.00

Submit Cancel

19 Feb 2014 © 2010-14 TrueTrust Ltd 14

Live Demo of TAAS

- The live demo is publicly accessible and is available from here
- <http://sec.cs.kent.ac.uk/demos>
- Select demo 5, Trusted Attribute Aggregation Service
- There are 3 demos available:
 - e-government, buying a car parking permit
 - e-business, online shopping for books
 - e-learning, downloading a peer-reviewed paper

19 Feb 2014

© 2010-14 TrueTrust Ltd

15

Adding FIM To OpenStack

- Protocol independent modular design
- Most functionality is provided by protocol independent code we have added to Keystone's core code
 - Adding/Retrieving IdPs to *enhanced Service Catalog*
 - *Attribute Issuing Policy* creation and enforcement - says which IdPs are trusted to issue which identity attributes to users
 - Creating and removing *temporary user entries* in Keystone
 - *Attribute Mapper* from IdP issued identity attributes into Keystone roles, projects and domains
 - *Delegating* permissions to IdP administrators to set up the attribute mappings and attribute issuing policies
- One plug-in module needed that handles the *Protocol Specific* features of federated login
 - IdP Request preparation
 - idP Protocol negotiation (optional)
 - IdP Response verification
- Obviously clients have to be tailored to support federated login

19 Feb 2014

© 2010-14 TrueTrust Ltd

16

Federated Authn Module Validation

- Four working implementations:
- SAML plugin based on pySAML – now an operational service in Brazilian academic network
- Keystone plugin – for federating multiple OpenStack/ Keystone installations together
- ABFAB plugin based on Moonshot software
- OpenID Connect plugin (written by PhD student in Brazil)

19 Feb 2014

© 2010-14 TrueTrust Ltd

17

Planned OpenStack April Release

- Keystone core developers decided to do a first quick fix for SAML only using Apache and mod_shib, and modifying the External authn method to pick up Remote_User and user's attributes as environmental parameters
- This will be working in time for the April release of OpenStack (codenamed Ice House)
- It will use the attribute mapping functionality from Kent's design/implementation to obtain the OpenStack roles and domains

19 Feb 2014

© 2010-14 TrueTrust Ltd

18

SCIM - System for Cross-domain Identity Management

- SCIM 1.0 was initially created to simplify user management in the cloud by defining a schema for representing users and groups and a REST API for all the necessary CRUD operations
 - Based on simplified LDAP schema (no inheritance), written in XML and JSON
- IETF WG will standardize SCIM 2.0 for creating, reading, searching, modifying, and deleting user identities and identity-related objects across administrative domains, with the goal of simplifying common tasks related to user identity management in services and applications

19 Feb 2014

© 2010-14 TrueTrust Ltd

19

SCIM Schema Examples

- | | |
|---|--|
| <ul style="list-style-type: none"> • XML of minimum user data <pre><User xmlns="urn:scim:schemas:core:1.0"> <id>2819c223-7f76-453a-919d-413861904646</id> <userName>bjensen@example.com</userName> </User></pre> | <ul style="list-style-type: none"> • JSON of minimum user data <pre>{ "schemas": ["urn:scim:schemas:core:1.0"], "id": "2819c223-7f76-453a-919d-413861904646", "userName": "bjensen@example.com" }</pre> |
|---|--|

19 Feb 2014

© 2010-14 TrueTrust Ltd

20

SCIM v1 API

- GET - Retrieves a complete or partial Resource
- POST - Create new Resource or bulk modify Resources
- PUT - Modifies a Resource with a complete consumer specified Resource (replace)
- PATCH - Modifies a Resource with a set of consumer specified changes (partial update)
- DELETE - Deletes a Resource

19 Feb 2014

© 2010-14 TrueTrust Ltd

21

Federated Authorization Management with Virtual Organizations (VOs)

- A VO is a security and collaboration context not exclusively associated with any one physical organization or site
 - Participating partners agree upon structure, rules and processes
 - A VO partner can be a single person, a group or an entire organization
- A VO has members that are assigned roles and/or attributes
 - Membership roles or attributes grant specific capabilities within a given VO as determined by each resource/service provider
- Partners participating in a VO contribute resources, i.e., data and services
 - They retain complete control over their own resources!
 - Access by VO members can be modified or revoked at any time by both the VO administrator and the resource administrator
- VOs enable federated, community clouds by being the Trusted Third Parties who assert user identity attributes, and who may authenticate users as well

19 Feb 2014

© 2010-14 TrueTrust Ltd

22

VOs and Federations

- A federation can contain many VOs
 - E.g. a national federation could host multiple VOs
 - IdPs in the federation may authenticate users and VOs provide the user's attributes to the SP – typically you cannot ask your organisation's IdP to add VO attributes to a user's corporate LDAP entry
- A VO can be a federation
 - All federation partners are partners in the VO. The VO decides how authentication will take place and identifies the users to SPs
- A VO can span multiple federations
 - To realize this, interconnected federations are needed first, such as eduGAIN. The federation IdPs will authenticate the users and the VO provides the identity attributes

19 Feb 2014

© 2010-14 TrueTrust Ltd

23

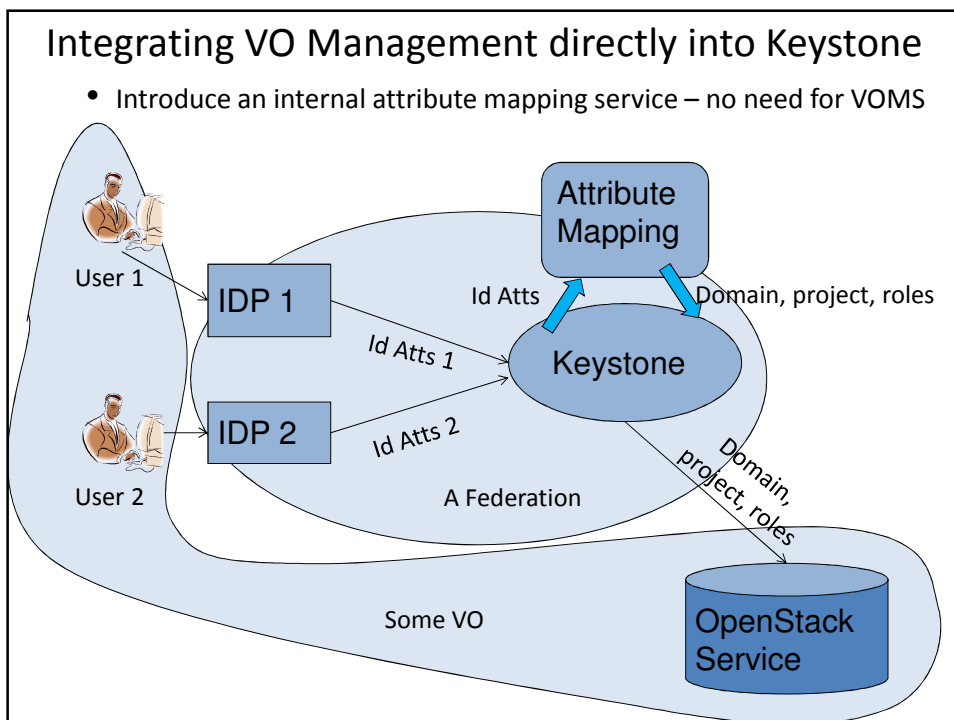
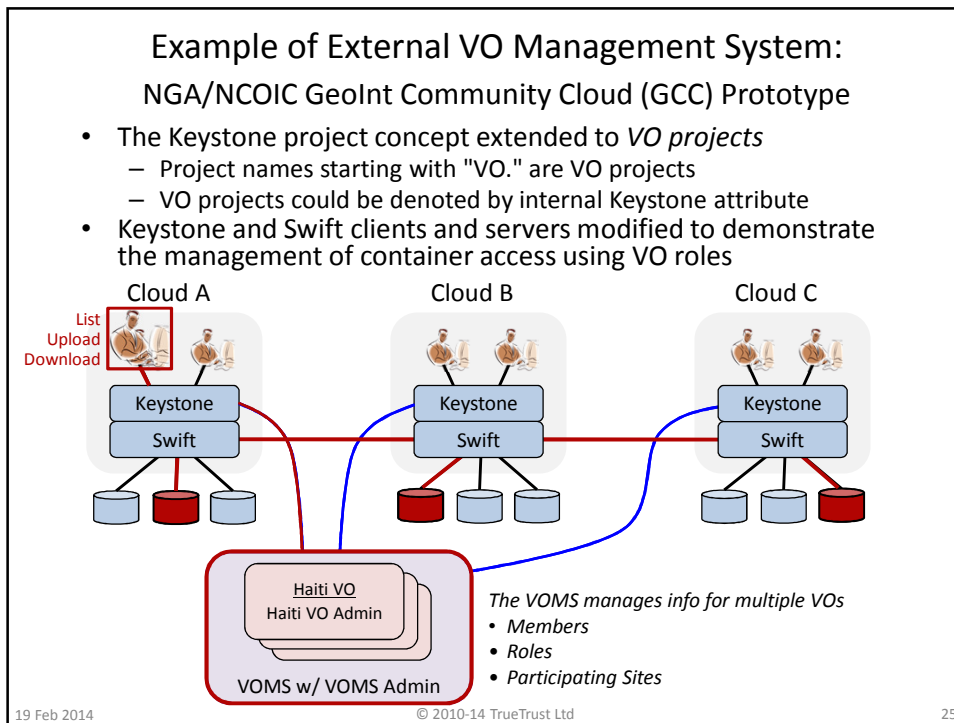
VO Management System (VOMS)

- Organisations do not usually allow groups of users to add attributes to their corporate LDAP service – reserved for HR and Comms depts
- So how can VOs be created and managed?
- Ans. Have a separate VO management service - VOMS
- VOMS is LDAP database with front end administrative interface allows VO admin to add roles and users
- API interface allows clients to retrieve a user's VO roles and attach them to the application request
- Applications can now grants access based on user's VO roles

19 Feb 2014

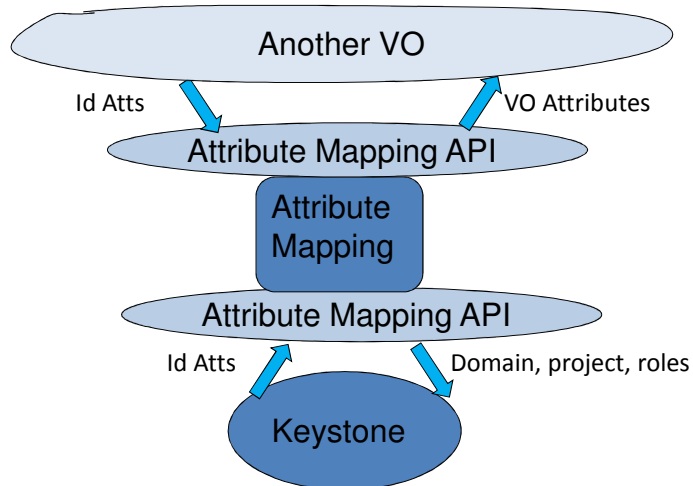
© 2010-14 TrueTrust Ltd

24



Extending Keystone to be a VO Manager

- Create an externally accessible Attribute Mapping API

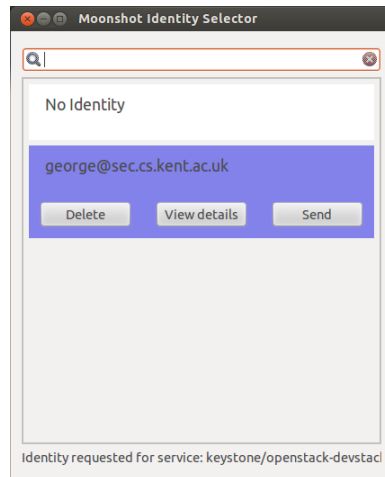


- Alternatively, Attribute Mapping could become a stand-alone OpenStack service

Key Design Issues for VOs in OpenStack

- How to store the VO attributes
 - As separate user entries with VO attributes (as per VOMS)
 - As a set of general mapping rules (as per attribute mappings)
- How to Integrate VOs with multiple clouds
 - Authenticating identity credentials from different *Identity Providers*
 - Aggregating IdP attributes with VO attributes
- External VOMS DB vs. Peer-to-Peer Keystone VO DBs
 - External VOMS easier to implement, quicker authz revocation process, but single point of failure
 - P2P doesn't rely on third party VOMS, not a single point of failure, but introduces consistency issue, and authz revocation takes longer
- Whether to check that user is a VO member or not
 - Carries an overhead (esp. if external VOMS DB) so when to avoid it?
- Ensure that VOs can be used by arbitrary application-level services
 - Database access, RSS feeds, any kind of standard services, e.g., geospatial tools: Web Map Service, Web Feature Service, Web Coverage Service, ...
- What should be at app-level vs. infra-level, i.e., what should be in Keystone
- Who manages the VOs ?
 - Each VO administrator (distributed) or the VOMS administrator (centralised)
- Infrastructure-level federation vs. application-level federation
- Scalability

ABFAB (Moonshot) User Experience



- User launches application client and connects to app server
- Identity Selector pops up
- User chooses which identity to use or adds a new one
 - Optional remember password
- System remembers choice and uses it automatically next time
 - User effectively gets Zero Sign On

19 Feb 2014

© 2010-14 TrueTrust Ltd

31

Inter-federations

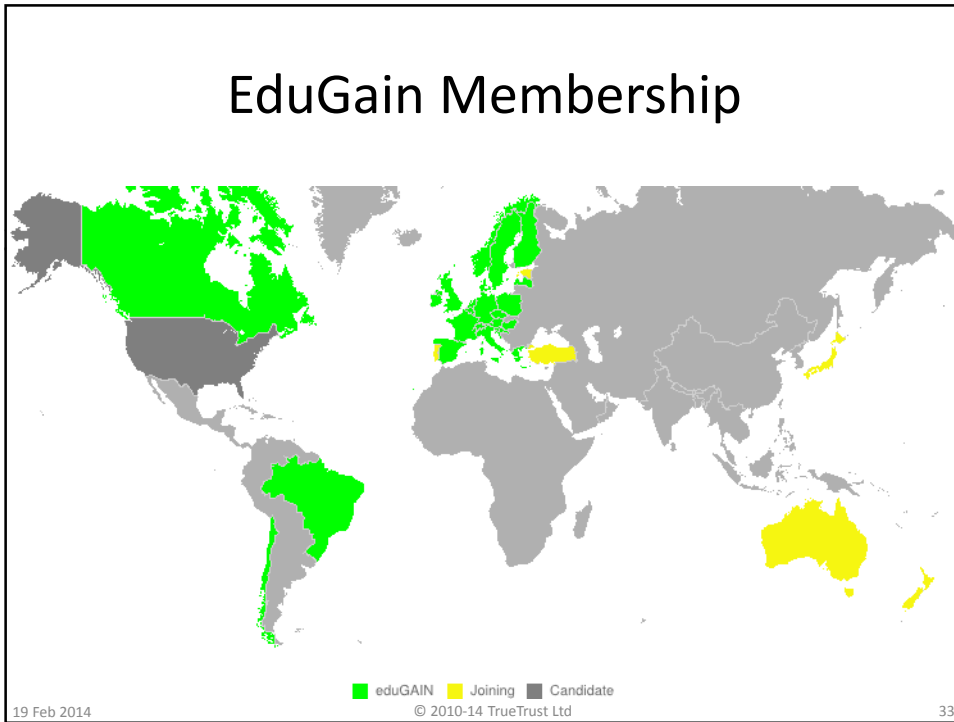
- Once you have an operational federation, one of the next steps to consider is linking your federation to other similar ones
 - E.g pan-European local government inter-federation
- EduGAIN – global effort to link national educational federations together
- Currently 23 countries are inter-connected
- 6 more are in the process of joining
- 1 further candidate member (USA)

19 Feb 2014

© 2010-14 TrueTrust Ltd

32

EduGain Membership



Any Questions

