



Identity Harmonisation

Nicole Harris
REFEDS Coordinator
GÉANT

<http://www.aai.edu.hr/dan2015.html>





“the voice that articulates the mutual needs
of research and education identity
federations worldwide”



Happy 10th Birthday REFEDS

[Read More..](#)

The mission of REFEDS (the Research and Education FEDerations group) is to be the voice that articulates the mutual needs of research and education identity federations worldwide. The group represents the requirements of research and education in the ever-growing space of access and identity management, working with and influencing the direction of other organisations on behalf of our participants.

REFEDS participants are from a wide range of backgrounds, but all share an interest in developing access and identity management technology, policies and processes. Many participants represent national identity federations and many come from National Research and Education Networks ('NRENS').



Support Documents



The REFEDS Community



Unlocking Attributes

The list of sponsoring organisations for 2015 is shown below.

Platinum Sponsors



Gold Sponsors



Silver Sponsors



Bronze Sponsors





ENTITY
CATEGORIES

FIM4R / SIRTFI

FEDERATION
TEMPLATES

VIRTUAL
ORGANISATIONS

MONITORING

SPECIFICATIONS
AND SCHEMAS



What do our users want?

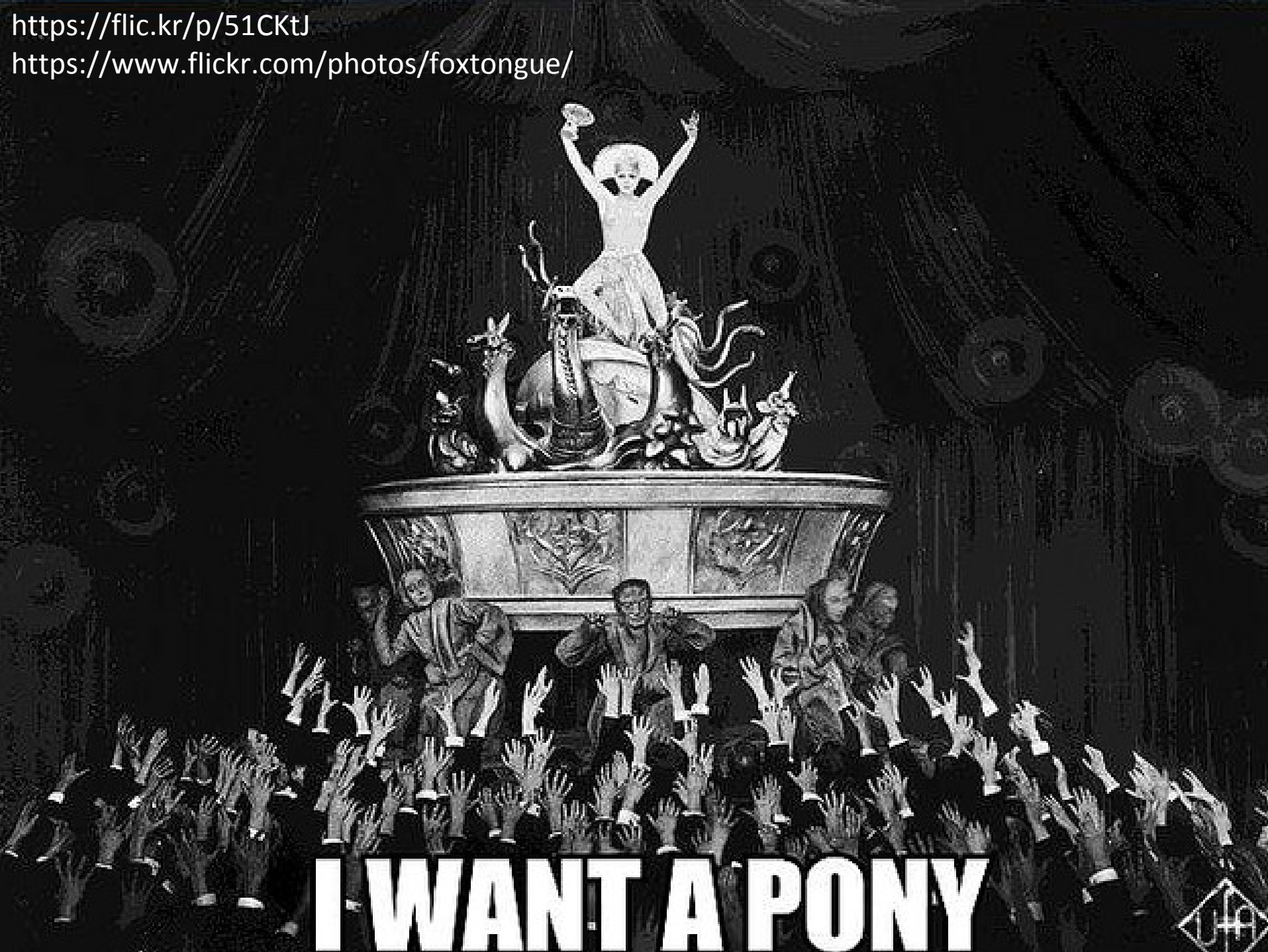
1. User Friendliness
2. Homeless Users
3. Different Levels of Assurance
4. Community based authorization
5. Flexible and scalable attribute release policies
6. Attribute Aggregation & Account Linking
7. Federation solutions based on open and standards based technologies
8. Persistent & Unique User Identifiers
9. User managed Identity Information
10. Up to date identity information
11. User groups and roles
12. Step up authentication
13. Browser and non-browser based federated access
14. Delegation
15. Social media identities
16. Integration with e-Government infrastructures
17. Service Provider Friendliness
18. Effective Accounting
19. Policy Harmonization
20. Federated Incident report Handling
21. Sufficient Attribute release
22. Awareness about R&E Federations
23. Semantically harmonized identity attributes
24. Simplified process for joining identity federation
25. Best practices for terms and conditions

What's new from our users?

1. User Friendliness
2. Homeless Users
3. Different Levels of Assurance
4. Community based authorization
5. Flexible and scalable attribute release policies
6. Attribute Aggregation & Account Linking
7. Federation solutions based on open and standards based technologies
8. Persistent & Unique User Identifiers
9. User managed Identity Information
10. Up to date identity information
11. User groups and roles
12. Step up authentication
13. Browser and non-browser based federated access
14. Delegation
15. Social media identities
16. Integration with e-Government infrastructures
17. Effective Accounting
18. Policy Harmonization
19. Federated Incident report Handling
20. Sufficient Attribute release
21. Awareness about R&E Federations
22. Semantically harmonized identity attributes
23. Simplified process for joining identity federation
24. Service Provider Friendliness
25. Best practices for terms and conditions

<https://flic.kr/p/51CKtJ>

<https://www.flickr.com/photos/foxtongue/>



I WANT A PONY





We don't normally communicate directly
with entities, but...



- How to use Federations more effectively:
<https://wiki.refeds.org/download/attachments/6619142/REFEDS.pdf>
- New Years Resolutions:
<https://wiki.refeds.org/download/attachments/6619142/Resolutions.pdf>

HOW TO USE FEDERATIONS

MORE EFFECTIVELY



HOW TO USE FEDERATIONS

MORE EFFECTIVELY

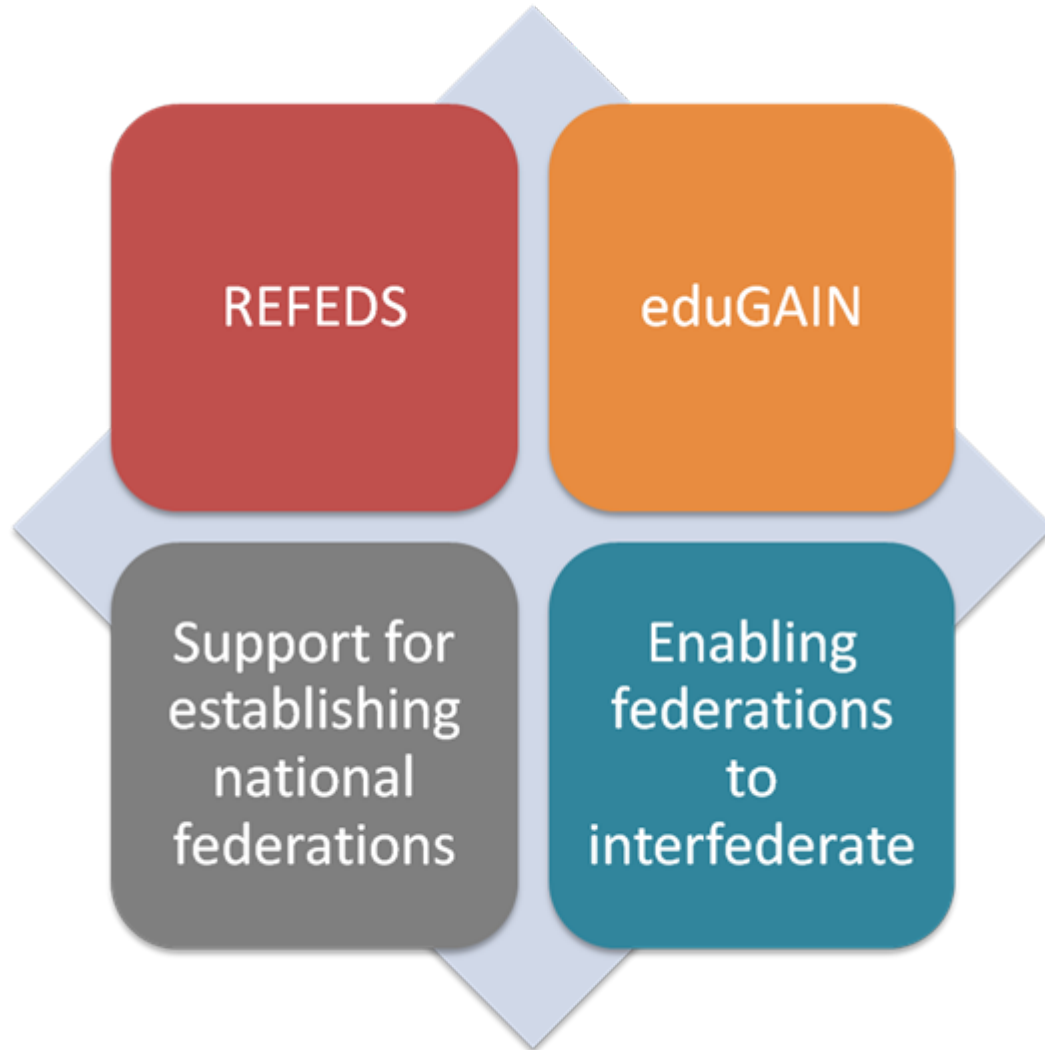
eduGAIN means there is no longer any need to join multiple federations. Choose your preferred home federation and ask them to export your metadata worldwide today.



<https://edugain.org>

Interfederate



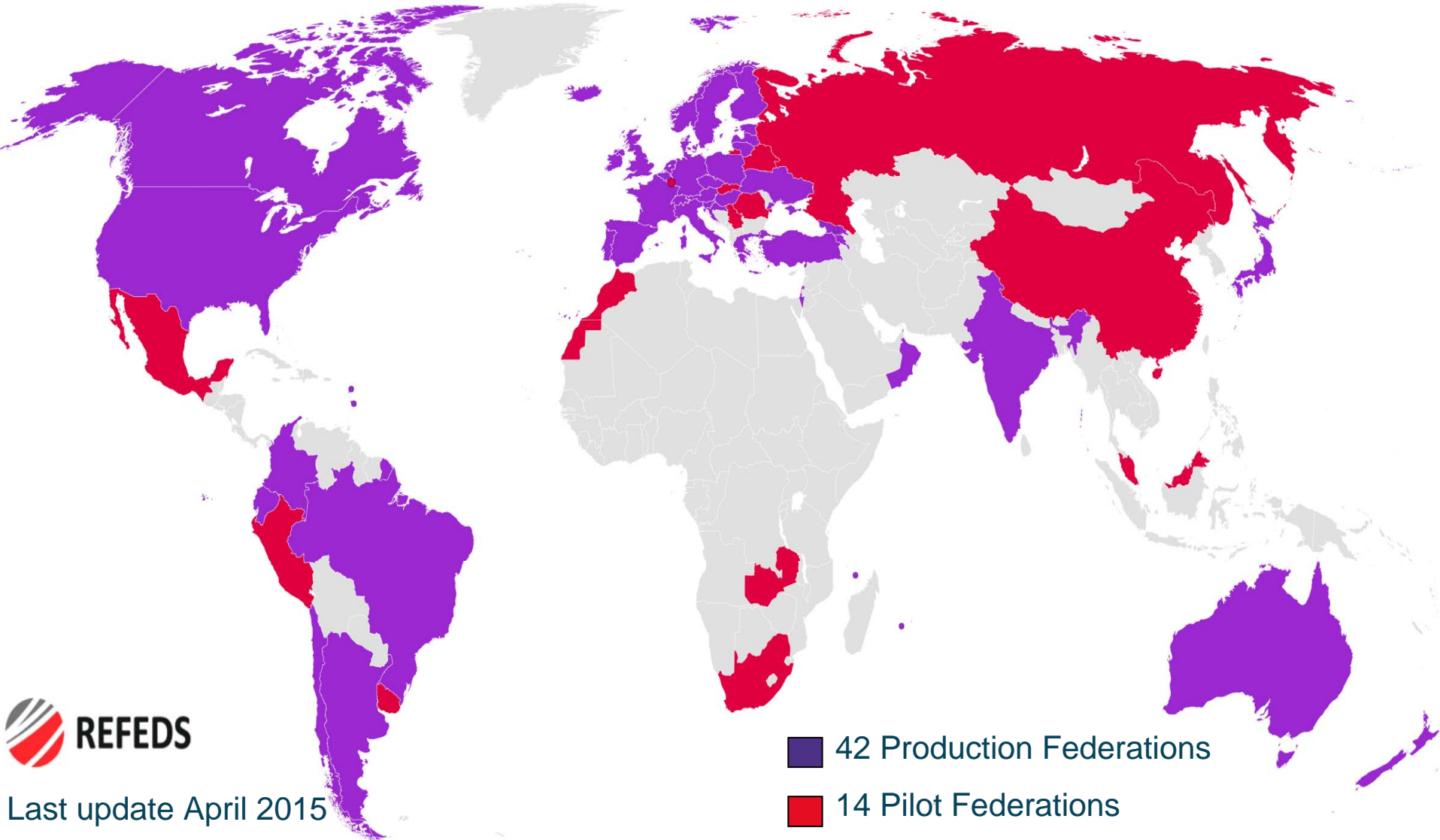


REFEDS

Lots of federations...

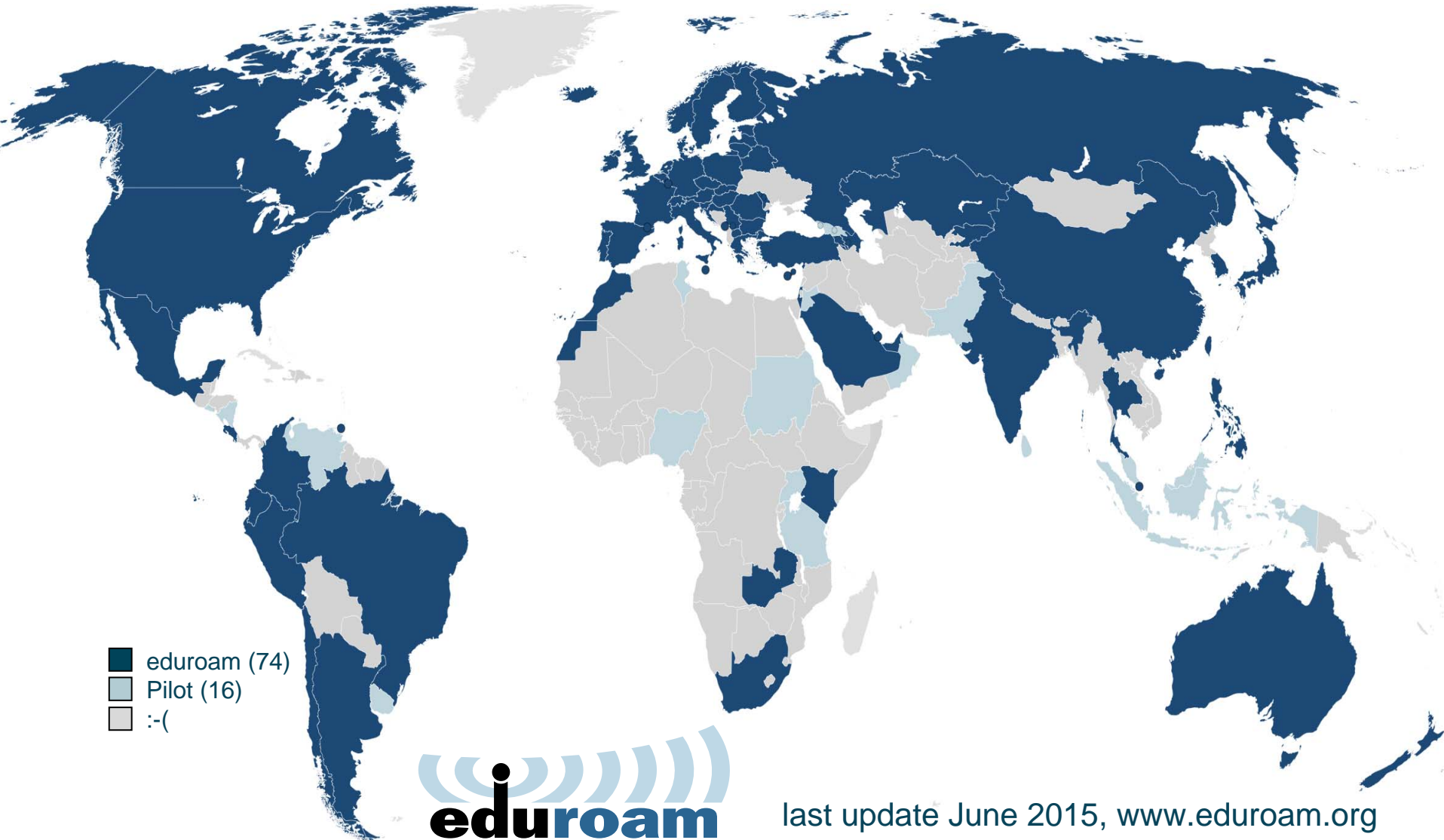


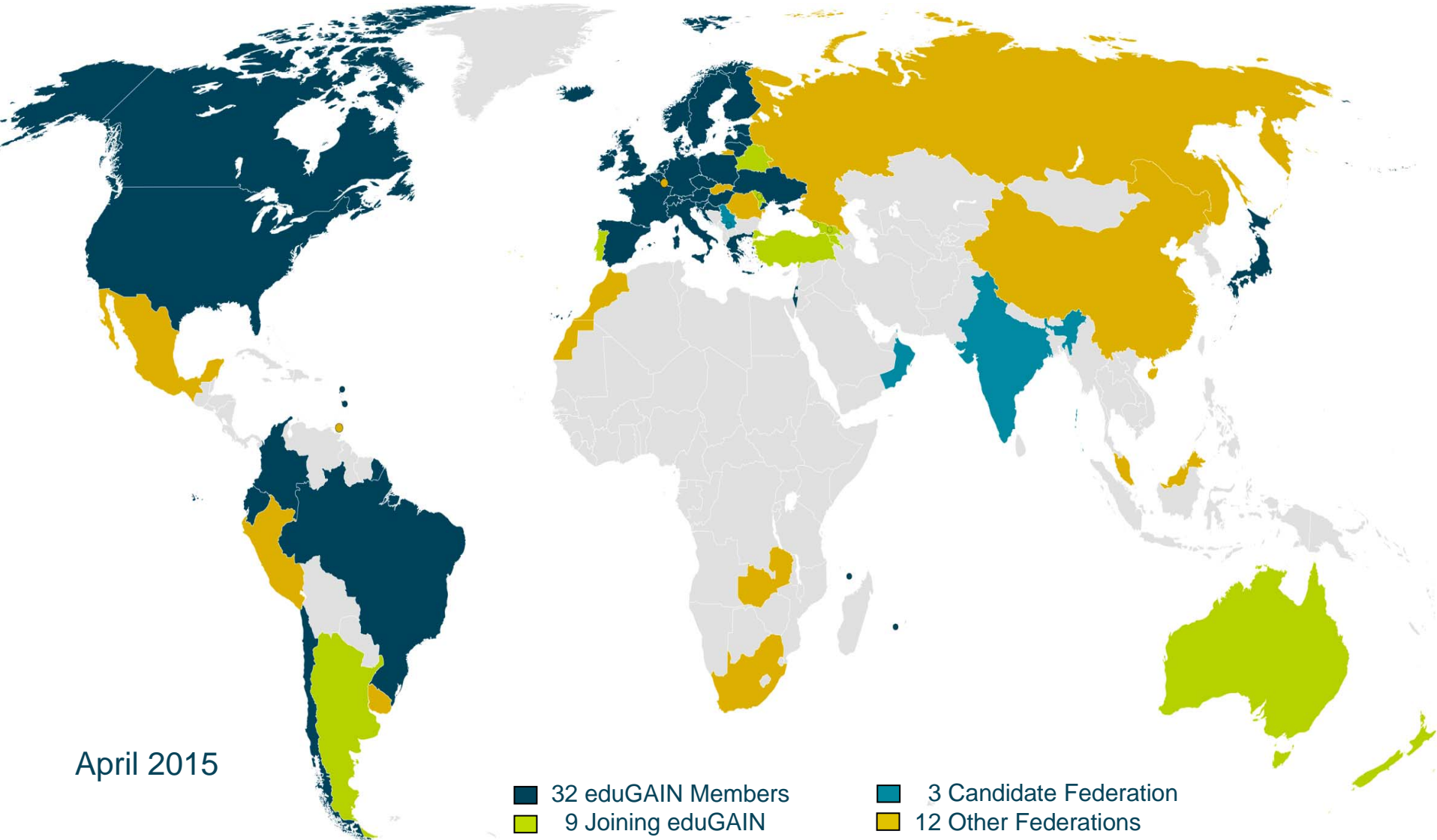
REFEDS Identity Federations: World Wide

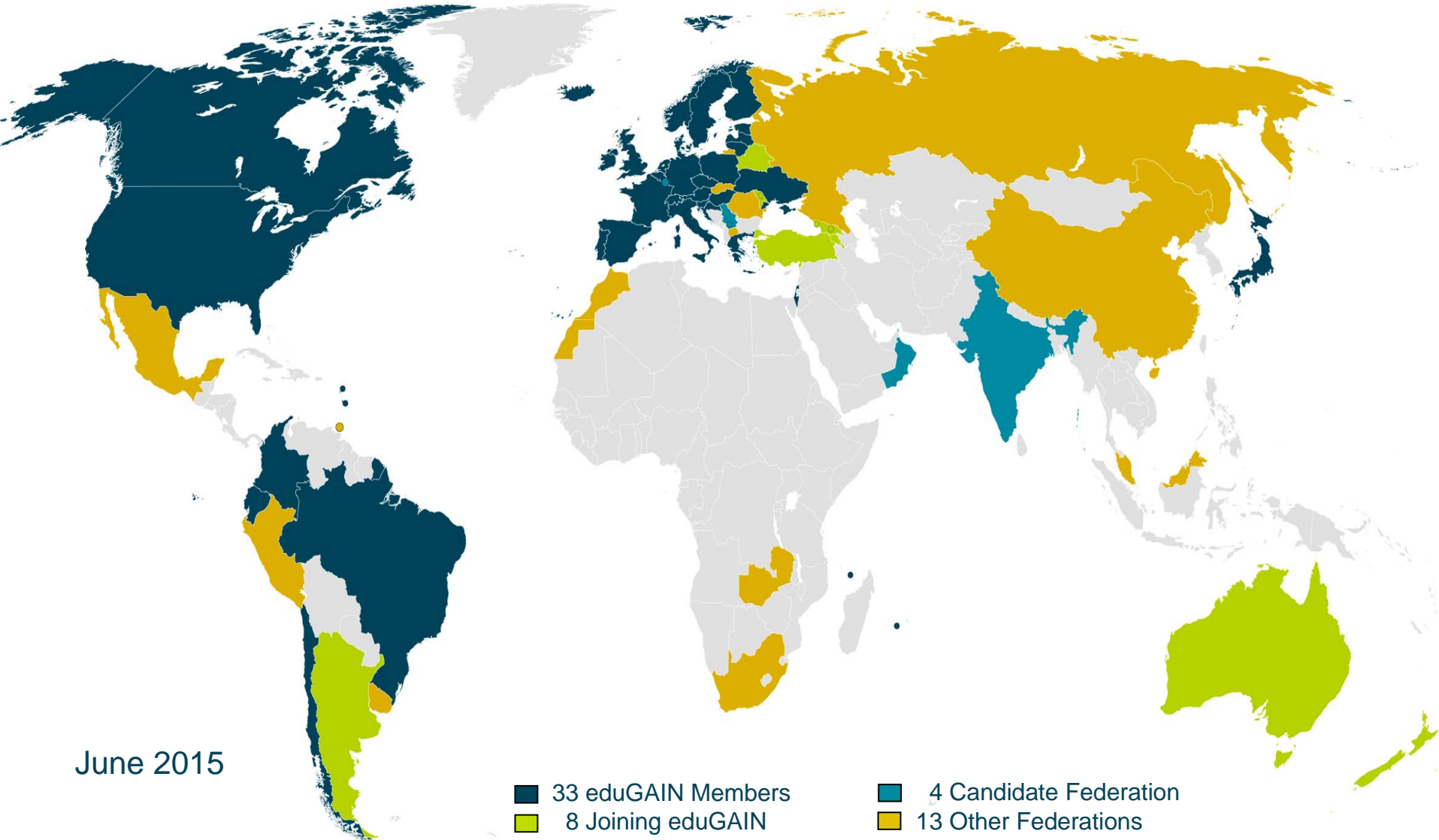


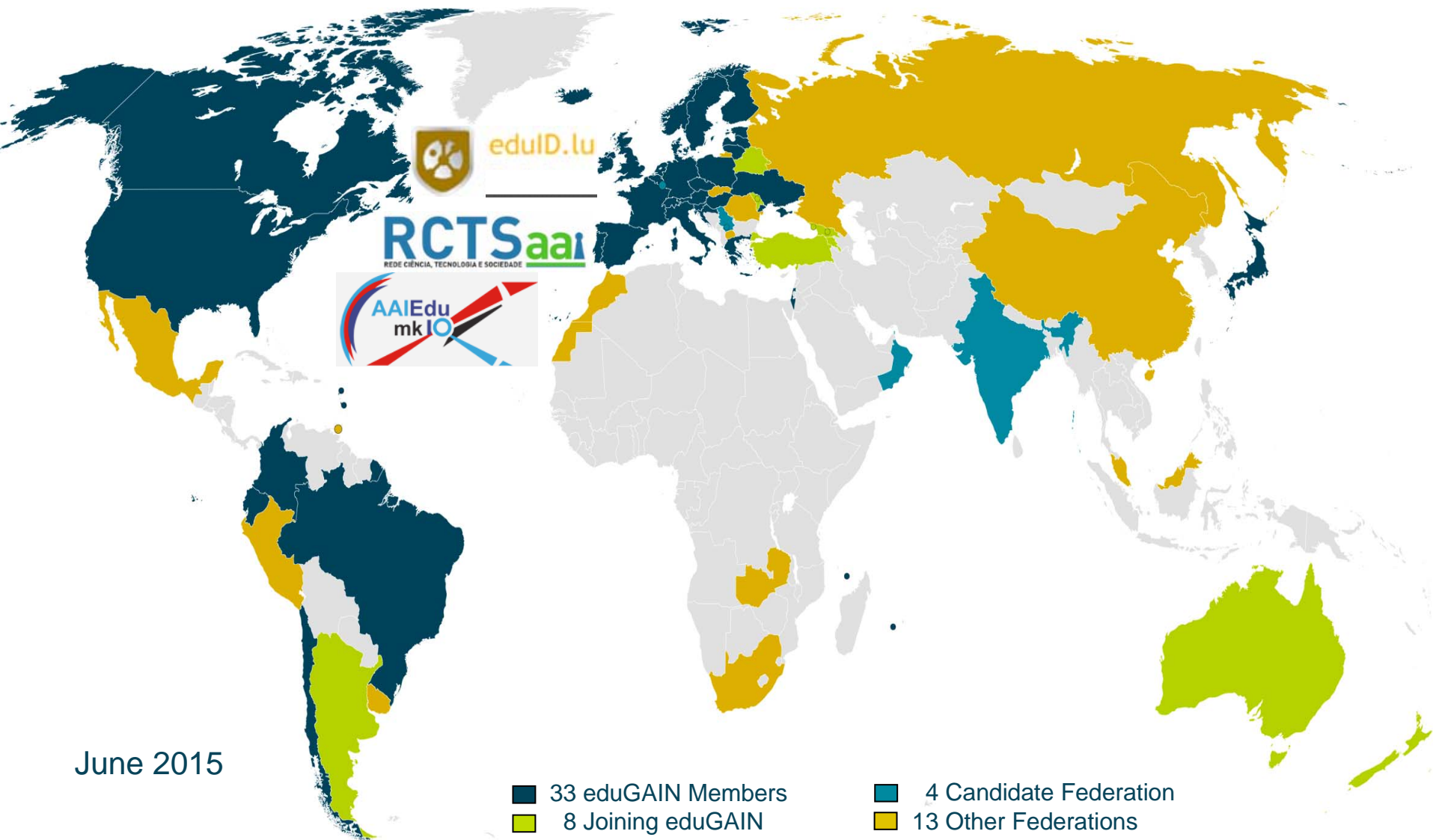


REFEDS eduroam Federations: World Wide











REFEDS

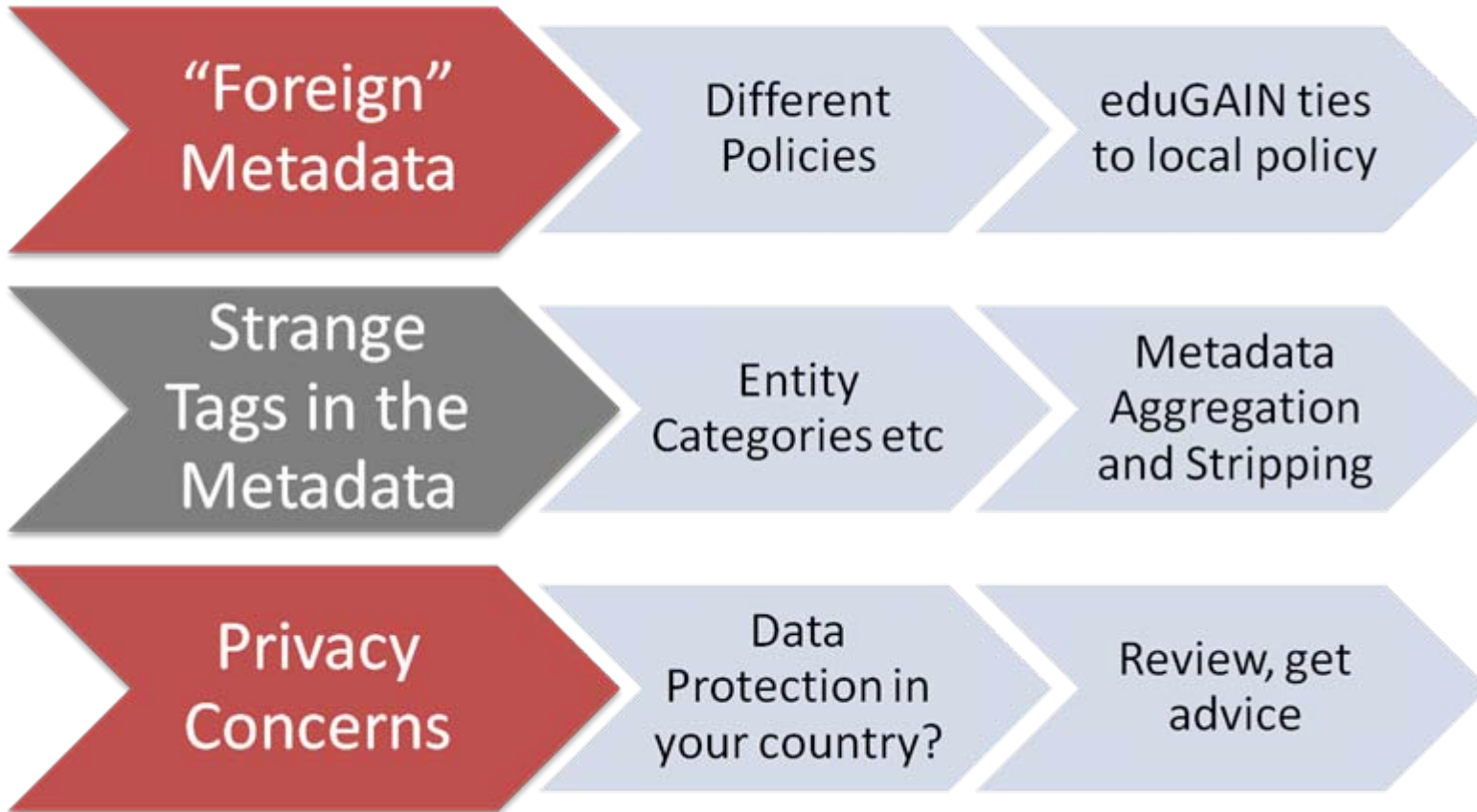
eduGAIN: Some Statistics

- **April 2011:** Official start of eduGAIN
- **Nov 2013: 21 Federations** are members (50%) , 5 joining
- **Apr 2014: 24 Federations** are members (51%) , 6 joining
- **April 2015: 32 Federations** are members (57%), 9 joining
- **June 2015: 33 Federations** are members (58%), 8 joining, 4 candidates

- **Entities: 1285 IdPs, 961 SPs (2244 in total)**
One IdP can represent for dozens of organisations and services depending on federation architecture => actual numbers are higher

- **Whole (academic) SAML landscape:**
56 Federations, 3007 IdPs, 6514 SPs (gathered from metadata)
Not all of them *need* to be interfederated, e.g. many internal SPs

Possible Issues?



HOW TO USE FEDERATIONS

MORE EFFECTIVELY

It is important that users are confident that their data is being well looked after. Services can sign-up to a federation "Code of Conduct" to declare that they look after personal data well.



<https://wiki.refeds.org/display/CODE/>

Look after
personal data



It is difficult for institutions to know the correct attributes to send to services to ensure privacy is preserved but services are usable. Entity Categories make these decisions easy for both institutions and services.



Help attributes flow

<https://wiki.refeds.org/display/ENT/>





What is an Entity Category?

- Entity Categories group federation entities that share common criteria.
- obliged to conform to the characteristics set out in the definition of that category.
- Can be SP or IdP tagged.
- a way to facilitate IdP decisions to release a defined set of attributes to SPs (scaling attribute release policies).
- Other use cases (see hide-from-discovery).
- Expressed as a SAML Attribute.

- Helps you tag entities to say certain things about them.
- “Hide from Discovery” = don’t display this IdP in your discovery service: <https://refeds.org/category/hide-from-discovery>.
- “Research and Scholarship” = this SP genuinely needs certain attributes to support research activity:
<https://refeds.org/category/research-and-scholarship>.
- “Code of Conduct” = this SP is self-declaring that it meets data protection standards IN EUROPE:
<https://wiki.refeds.org/display/CODE/>.

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://service.example.com/sp">
<Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
<mdattr:EntityAttributes xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
<saml:Attribute
Name="http://macedir.org/entity-category"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue>http://refeds.org/category/research-and-
scholarship</saml:AttributeValue>
</saml:Attribute>
</mdattr:EntityAttributes>
</Extensions>
...
</EntityDescriptor>
```



Can I Release Attributes?



<https://wiki.refeds.org/display/ENT/Guidance+on+justification+for+at+tribute+release>



CONSENT	The data subject has unambiguously given his consent.
CONTRACTUAL	Processing is necessary for the performance of a contract to which the data subject is party.
LEGAL OBLIGATION	Processing is necessary for compliance with a legal obligation to which the data controller is subject.
VITAL INTEREST	Processing is necessary in order to protect the vital interests of the data subject.
PUBLIC INTEREST	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.
LEGITIMATE INTERESTS	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed.

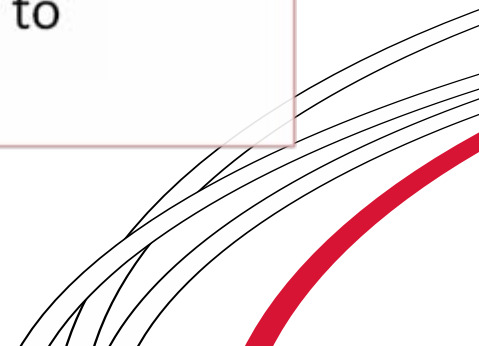
STEP ONE

- Check that Legitimate Interests is the best approach.

STEP TWO

- Qualify the legitimacy of the request – lawful, clearly articulated, real need.

STEP THREE

- Determine whether the processing is necessary to achieve the goal.
- 

STEP FOUR

- Balance the data controller's needs against the interests of the subjects.

STEP FIVE

- Identity safeguards you can put in place (tech design etc).

STEP SIX

- Demonstrate (publish) compliancy.

STEP SEVEN

- Allow the user to opt-out.
- 

HOW TO USE FEDERATIONS

MORE EFFECTIVELY



Metadata is the life-blood of identity federations and if yours is out of date, your users may not reach their destination. Make sure your federation has an organisational name, organisational description and your logo in your metadata.



Update your
discovery data

<https://discovery.refeds.org>





<https://discovery.refeds.org/>





★ ★ 2016 ★ ★

NEW YEAR'S

RESOLUTIONS

TOP 6 RESOLUTIONS

January is a great time for New Year's Resolutions.
Why not make these for your federated entities today?





REFEDS



01 Implement Research and Scholarship Entity Category



02 Upgrade your Software



03 STOP Using SAML 1



04 Join eduGAIN



05 Improve Discovery



06 Use the Code of Conduct



- Help us design our workplan:
<https://wiki.refeds.org/display/WOR/2016+Work+Plan+Preparation>
- Participate:
<https://refeds.org/about/refeds-participants-agreement>

<https://flic.kr/p/hoMcw>

<https://www.flickr.com/photos/marcusramberg/>

