

Discovery Best Practice

- [Discovery Background](#)
- [Why No Central Brand?](#)
- [Guide for SPs](#)
- [Guide on MDUI](#)

Discovery Background

In 2009 / 2010 REFEDS [ran a working group](#) looking at ways in which the discovery process for federated access could be improved. The group initially focused on the idea of creating an internationally recognised brand that could sit alongside social logins such as Facebook or Google. Although [initial reports](#) were favorable as to the benefits of such an approach the group concluded that there would not be enough buy-in for such a logo and significant uptake would be needed to make this work. REFEDS endorsed the use of the wording "institutional login" or "organisational login" for discovery instead of a brand, highlighting the importance of the organisation as the core trust focus in the process.

REFEDS decided to instead develop a best practice guide for Service Providers to show how discovery could be well implemented.



Access the [REFEDS Discovery Best Practice Guide for Service Providers](#) here.

Service Providers are encouraged to use software that uses [MDUI](#) information in SAML Metadata to drive branding.

Why No Central Brand?

Many people have asked why the central brand was not implemented despite the positive recommendations from the report. Some of the main reasons are:

No.	Issue	Commentary
1.	Phishing	One of the main reasons for not introducing another brand is phishing concerns. A logo would be easy to copy and the owners would have little control over it. As the click would not always take the user to one central place but to a multitude of different WAYFs it would be difficult to prevent misuse. Users are typically advised to look for consistency of branding as they go through the login screens but as the federated approach is highly decentralised there would be little ability to control the flow - so the "eduid" brand would not necessarily appear on the login page at the institution, on the software being used for the WAYF etc. Unless consistency could be ensured across the screens there would be a security risk.
2.	No centralisation	<p>Drawing on from the argument above, federated identity is very different from the Facebook or Google approach. Although described as a federated approach, these are essentially single identity providers and the links go to the same IdP each time. Even locally "eduroam" is a very different thing - it is a single service delivery model so it is easier to enforce some level of control, where as SAML federations are many to many relationships.</p> <p>The federated approach used by R&E goes to thousands of different IdPs that do not necessarily have any relationship with the central brand - the model does not map in the same way.</p>
3.	Brand level	<p>There are many many competing brands in this space and different groups want to be able to brand differently. Many federations have pushed their own local brand from the beginning and want to keep this. Others believe in no branding apart from the drawn from MDUI which correctly allows the user to identify with the IdP and SP brands as appropriate. Groups are clustered differently and often have an agenda to push a brand - eduGAIN could be seen as an attractive brand, but it currently only serves a very small percentage of the traffic that goes through R&E federations. REFEDS could also have a brand, ORCID could have a brand etc. etc. Among publishers it is still common to see a link to "shibboleth" despite the fact that this has never been recommended by the shibboleth team.</p> <p>Another issue would be who would own the brand? REFEDS would still be willing to take on this role but it would need to be a funded activity.</p> <p>Specific issues with brands:</p> <ul style="list-style-type: none">• eduID has now been taken and used in a different way by federations.• eduGAIN does not have enough coverage and would never represent all traffic and takes away from the concept of keeping eduGAIN as a lightweight metadata exchange service only. There are currently only 13% of worldwide SPs in edugain, and this goes down to 3% if you take out the UK SP traffic.
4.	Institution as Brand	Federations highlight the user's relationship with their organisation as one of the benefits of using the federation model and pushes the trust concept of access via the organisation. The organisational brand should be the main brand in the workflow. Other branding approaches take away from this concept.
5.	Buy In	For this approach to be successful, a very high level of buy-in would be needed due to the issues highlighted above. To date, there has not been enough evidence that all federations would be willing to adopt this approach. Getting federations to agree on consistent common practice has proven to be almost impossible.

6.	Central Support	If a brand such as "eduid" was to be used, users would naturally think this brand controlled the whole process and would want to complain when "eduID" was broken. A central support team would be essential, as would links to the helpdesks for all the federations in order to pass off queries. This would create a new overhead that is currently not funded via any source.
7.	No a full solution	A branded button may help users quickly find the right place to be but the "discovery" process still needs to carry on and the right IdP found. Bad discovery practice will still continue from this point, the button doesn't solve all the issues with bad implementation.

Guide for SPs

REFEDS has created a [Discovery Guide for Services Providers](#) looking to implement IdP discovery on their sites.

Guide on MDUI

REFEDS has prepared advice on using MDUI (Metadata for User Interfaces):

- [MDUI Advice.](#)
- [MDUI Federation Recommendations.](#)
- [MDUI Software Recommendations.](#)