Federated Authentication for E-Infrastructures

A growing challenge for on-line e-infrastructures is to manage an increasing number of user accounts, ensuring that accounts are only used by their intended users, that users can be held accountable for any misuse, and that accounts are disabled when users are no longer entitled to use them. Users face a similar challenge in managing multiple authentication credentials for different on-line services. One option, which may provide more efficient authentication for e-infrastructures and a better experience for users, is to build on the account management systems and processes already provided by users' home universities or colleges. Federating authentication in this way is already commonly used to gain access to networks (eduroam[1]) and electronic publications (UK Access Management Federation[2]). E-infrastructures based on X.509 proxy certificates can implement federated login to certificate stores or issuers, for example using the SLCS[3] or IOTA[4] profiles. Janet, a part of Jisc, is currently piloting technologies and processes that make federated authentication suitable for a wider range of e-infrastructure services. This paper therefore identifies the authentication services likely to become available to e-infrastructures through federation and considers the benefits they may bring.

What does it look like?

For the user, federated authentication should look almost the same as their existing login to an e-Infrastructure, but instead of having to remember a username and password for each service, they use their familiar username and password from their home organisation. The only difference is that the user may need to indicate to the service which that home organisation is: depending on the technology that may be done by appending it to the username (as with eduroam: *johns@camford.ac.uk*), selecting it through a drop-down menu (common with web federation: *Camford University*), or another simple interface. The password is not disclosed to the e-infrastructure: instead it is routed directly to the user's home organisation where it can be checked both for correctness and currency. The e-infrastructure receives confirmation that the user has authenticated successfully and is provided with a unique identifier for that user that can be used to link the authentication to the user's resources and permissions on the e-infrastructure.

What assurance does it offer?

Any authentication system, whether local or federated, needs to provide the owners of services and information it protects with the assurances of identity and accountability they require. In particular, service and information owners need confidence that an account will remain linked to the same individual; that the individual can be held accountable for any misuse of services or information; and they will learn of relevant changes to that individual's status. By using federated authentication backed by appropriate agreements, an e-infrastructure provider knows

[1] http://www.eduroam.org/

[2] http://www.ukfederation.org.uk/

[3] http://www.igtf.net/ap/slcs/

[4] http://www.eugridpma.org/guidelines/IOTA/

that it has the same assurance on these points as the home organisation relies on for its own local needs, since both are using the same technologies, processes and policies. The following sections consider what assurances are likely to be available from universities and colleges who participate in existing federated authentication schemes.

Knowledge of user

Universities and colleges will generally know the identities of their users to at least level 2 (and sometimes higher) on the UK Government's Identity Proofing scale as a result of their normal relationship with the individual. This will, for instance, involve payments either to (employees) or from (students with loans; accommodation costs etc.) an individual's account with a financial institution, as well as checking evidence of academic activities over previous years.

According to the Government's Good Practice Guide (GPG-45): *"A Level 2 Identity is a Claimed Identity with evidence that supports the real world existence and activity of that identity. The steps taken to determine that the identity relates to a real person and that the Applicant is owner of that Identity give sufficient confidence for it to be offered in support of civil proceedings."*[5]

Level 2 identities are considered equivalent across various national and international schemes including STORK, ISO 29003 and NIST 800-63.[6]

Strength of credential

Virtually all UK universities and colleges issue individual usernames and passwords to users of their general education and research services. Good practice guidance, technical controls on password complexity and the issuer's strong interest in ensuring that authentication to its own systems and data remains secure should ensure that these, too, match the authentication requirements of a Level 2 identity under GPG-45. Stronger, multi-factor, authentication systems may sometimes be used by universities and colleges for individual users with access to sensitive systems and data, but these are unlikely to be available through federation at present.

Information available

Most federated authentication systems used in research and education have been designed to protect the privacy of the user, while maintaining accountability through policies (see next section). By default they may only provide confirmation that the user is a current member of the organisation together with a persistent unique identifier that can be used to associate the user with a local account that holds information and access permissions. For e-infrastructures that require users to pre-register giving personal details, this real world information can be reliably linked to the on-line account using the persistent identifier. This avoids the difficulties of trying to link accounts based on what may be a common personal name, or of attempting to link using e-mail addresses which only works if the user chooses the same e-mail address to present to both their home organisation and the e-infrastructure.

Where services do not require prior authentication, but can be used merely on presentation of an on-line identity, the service may ask the user to volunteer additional personal information. Services should not rely on

[5] GPG-45, para 20, page 11 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/271266/GPG_45_Identity_proofing_and_verification_of_an_individual_-_issue_2.2_December_2013.pdf)

[6] GPG-45, para 8, page 6

the accuracy of this information, since it will be self-asserted, but for options such as preferred form of address or e-mail address for communication, this may in any case be the best way to gather users' preferences. For example, a user may be known to an on-line community by a different form of name from the formal name recorded by their employer. Services should not need to gather personal information such as name merely to enforce their policies since, under federation agreements, that can be done more effectively by the home organisation.

For on-line services that involve individuals interacting with one another using verified names and e-mail addresses, identity providers may be willing to release this information if the benefit of doing so is clear and the risk (for example under data protection legislation) acceptably low. A set of rules for research collaboration services has been developed within the Research and Education Federations (REFeds) community[7]. Identity providers may be more willing to release personal data to service providers that satisfy these rules, so service providers may consider becoming early adopters of this category.

Accountability policies

A significant advantage of federated authentication is the possibility of involving the user's home organisation in holding them accountable for any misuse. Acceptable Use Policies form part of most organisations' contracts with their employees and students; sanctions for breaching such policies can have much greater impact than those an e-infrastructure might be able to impose on its own. One of the key requirements for service providers to be willing to trust home organisations to perform authentication on their behalf, is that those home organisations also agree to enforce service providers' policies on the users they authenticate, in particular to deal effectively with complaints from service providers. UK universities and colleges who are members of the eduroam or UK Access Management Federations already implement these federated accountability rules; those who provide visitor network services within the eduroam federation are also used to relying on them to protect their own organisations' services and reputation.

Comparing federated and local authentication

The following table compares the options available to e-infrastructure providers by using federated authentication against infrastructures providing their own authentication services.

[7] https://refeds.org/category/research-and-scholarship/

janet

Knowledge of User	Federated identity providers have knowledge of their users gathered during a period of employment or education. This will normally include evidence of financial and educational histories from private information. Identity providers are required to stop authenticating to external services when the user ceases to be a current member in good standing.	E-infrastructure service providers may be able to identify users from publication history or, in some cases, community knowledge. Face-to-face identification is likely to be expensive for on-line services. E-infrastructure providers are unlikely to discover when a user leaves their current organisation.
Strength of Credential	Federated identity providers are likely to use static username/password for most users. These credentials will be managed and used to a sufficient standard to protect access to the organisation's own internal services and information. Misuse of credentials may be detected on any of the systems where they are used. Where e-infrastructures involve a group management stage this may be used to impose additional duties on each user before adding them to groups. For example, users could promise to choose and use their credentials in accordance with the group's best practice.	E-infrastructure service providers that issue their own authentication credentials may be able to impose more precise technical requirements, for example on password complexity or certificate strength, but have fewer opportunities to detect misuse. Users may be less motivated to protect single-purpose credentials, since losing them will not affect their access to other services. E-infrastructure providers needing multi-factor authentication are likely at present to have to either issue tokens to users themselves or enter into an agreement with either their users' home organisations or a third party identity provider to do so.
Information Available	Federated identity providers are likely by default to provide a unique identifier for the user and their current status with the organisation. This may be linked to information gathered by the e-infrastructure provider from its own user registration process. Identity providers may be willing to release additional current information about the user (if they have it) to individual services or, in future, to registered research collaboration services.	E-infrastructure service providers may be able to obtain self-asserted information from their users, or from their collaborators. Where use of the service requires pre-registration, information from that process may also be available. Ensuring this information is kept up to date is likely to be challenging.
Accountability	Federated identity providers agree to enforce the policies of other federation members. Such enforcement can cover a wide range of sanctions, from informal face-to-face warnings to dismissal.	E-infrastructure providers may be able to impose limits on a misuser's activities on the service, or ultimately to ban them. Communication with the user is likely to be limited to what is possible remotely and that the user is willing to accept.

janet

What if it doesn't meet my requirements?

Unaffiliated users

Although national research and education federations are increasingly linked through the eduGAIN[8] system, some e-infrastructures may wish to include users who are not staff or students at any federation member organisation. For these users, e-infrastructures may choose to issue their own credentials (with the characteristics in the right hand column of the table above), or they may use various "self-service" authentication services such as social networks. These will have some of the characteristics of federated authentication providers, for example on strength of credential and information available, but are unlikely to have strong knowledge of the user's identity or to play any part in user accountability. E-infrastructure providers are still likely to need to address these issues themselves.

Higher assurance requirements

A number of "higher assurance" requirements have been requested by service providers, including stronger authentication credentials; more, or more strongly verified, information about users and legal liability for errors. Discussions are continuing to determine whether there is a set of higher assurance requirements that would be deliverable by sufficient identity providers and of value to sufficient service providers for a federated approach to be effective. One significant challenge is to ensure that joining such a higher assurance federation agreement benefits both service provider and identity provider members since it is likely to involve identity providers taking on duties and liabilities that they do not appear to require for their own internal risk management.

Some "higher assurance" features, such as multi-factor authentication, may be available from external identity providers outside federation agreements (as discussed in the previous section on unaffiliated users). However, the conditions of these services are unlikely to be negotiable so using them is likely to involve trade-offs for service providers: for example, accepting lower individual accountability in exchange for a higher-strength authentication method.

Conclusion

Federated authentication is already in production use globally for guest network access, and nationally for web-based research and education services. These experiences suggest that federated authentication could also have significant benefits for many e-infrastructures, particularly as these grow in scale and managing user accounts becomes more costly for both providers and users.

Federated authentication for e-infrastructures is currently being piloted using both web and other protocols, to determine how these requirements differ from existing production services. During these developments it is likely that e-infrastructures will need to work with federation operators and identity providers to achieve technical, operational and regulatory compatibility. Identifying a common set of requirements for e-infrastructure federation, as has already been done for international network access and national web federations, should reduce this need at least for those e-infrastructures that share the common requirements. Even for pilot sites, however, the benefits of federation should increase over time as the initial adoption costs are recovered through significantly reduced on-going operational and regulatory costs in future.

[8] A GÉANT funded service that allows national federations to share relevant information (interfederate).