Internet Engineering Task Force (IETF)
Request for Comments: 7832
Category: Informational
ISSN: 2070-1721

R. Smith, Ed.
Jisc
May 2016

Application Bridging for Federated Access Beyond Web (ABFAB) Use Cases

Abstract

Federated identity is typically associated with web-based services at present, but there is growing interest in its application in non-web-based contexts. The goal of this memo is to document a selection of the wide variety of these contexts whose user experience could be improved through the use of technologies based on the Application Bridging for Federated Access Beyond web (ABFAB) architecture and specifications.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7832.

Copyright Notice

Table of Contents

1. Introduction

Federated identity facilitates the controlled sharing of information about people (a.k.a. "principals"), commonly across organizational boundaries. This avoids redundant registration of principals who operate in and across multiple domains, both reducing the administrative overhead for the organizations involved and improving the usability of systems for the principal. Simultaneously, it can also help address privacy-related concerns, along with the regulatory and statutory requirements of some jurisdictions.

The information that is passed between organizations may include authentication state and identity information that can be used for many purposes, including making access management decisions. A number of mechanisms support the transmission of this information for web-based scenarios in particular (e.g., the Security Assertion Markup Language (SAML) [OASIS.saml-profiles-2.0-os]), but there is significant interest in the more general application of federated identity to include non-web use cases. This document enumerates some of these use cases, describing how technologies based on the ABFAB architecture [RFC7831] and specifications could be used.

2. Context of Use Cases

The use cases described in this document are a result of work led by Jisc, the operator of the United Kingdom's education and research network, responding to requirements from its community. These use cases have also been augmented by various inputs from the IETF community.

The ABFAB architecture and specifications enables authentication and authorization to occur across organizational boundaries. For many applications, principals need not have pre-instantiated accounts that their federated identity maps to before their first visit to that application; the application can perform this process on the fly. In cases where such accounts are required for particular applications, the pre-provisioning process is out of scope; the ABFAB technology assumes that any such requirements have already been fulfilled. Standards-based work of note that would assist with this pre-provisioning of accounts includes the standards and specifications produced by the IETF SCIM working group.

3. Use Cases

This section describes some of the various potential use cases where technologies based on the ABFAB architecture and specifications could help improve the user experience; each includes a brief description of how current technologies attempt to solve the use cases and how this could be improved upon by ABFAB implementations.

3.1. Cloud Services

Cloud computing is emerging as a common way of provisioning infrastructure services in an on-demand manner. These services are typically offered as one of three models:

- o General infrastructure services such as computing power, networks, storage, and utilities ("Infrastructure as a Service", or IaaS);
- o Software stacks or platforms such as database servers, web servers, and application runtime environments ("Platform as a Service", or PaaS);
- o Common application software such as email, shared storage, business applications such as Customer Relationship Management (CRM), or scientific applications ("Software as a Service", or SaaS).

In many cases, the provisioned cloud infrastructures and applications need to be integrated with existing infrastructure of the organization, and it is of course desirable if this could be achieved in a way that allows business or scientific workflows to act across infrastructure -- both across the cloud and in the local infrastructure -- in as seamless a manner as possible.

There are two main areas where federated access fits in cloud computing:

- Using federation to help mediate access to cloud-based application services (e.g., cloud-provided email or CRM systems);

- Using federation to help mediate access to the management of cloud-based infrastructure services.

3.1.1. Cloud-Based Application Services

Many organizations are seeking to deliver services to their users through the use of providers based in the "cloud". This is typically motivated by a desire to avoid management and operation of commodity services that, through economies of scale and so forth, can often be delivered more efficiently by such providers.

Many providers already provide web-based access using conventional federated authentication mechanisms -- for example, outsourced email provision where federated access is enabled using "webmail" applications where access is mediated through the use of SAML [OASIS.saml-profiles-2.0-os]. This use of federated authentication enables organizations that consume cloud services to more efficiently orchestrate the delivery of these services to their users and also enables single sign-on to the services for these users.

Frequently, however, users will prefer to use desktop applications that do not use web (i.e., based on HTTP) protocols. For example, a desktop email client may use a variety of non-web protocols, including SMTP [RFC5321], IMAP [RFC3501], and the Post Office Protocol (POP) [RFC1939]. Some cloud providers support access to their services using non-web protocols; however, the authentication mechanisms used by these protocols will typically require that the provider has access to the user's credentials -- i.e., non-federated. Consequently, the provider will require that users' credentials are regularly synchronized from the user organization to the provider, with the obvious overhead this imparts on the organization along with the obvious implications for security and privacy, or else be provisioned directly by the provider to the user.

The latter approach of directly provisioning accounts may be acceptable in the case where an organization has relationships with only a small number of providers, but this approach may become untenable if an organization obtains services from many providers. Consequently, any organization with a requirement to use non-web protocols would prefer to make use of the credentials that they have already provisioned their users with, and to utilize federated authentication with non-web protocols to obtain access to cloud-based providers.

ABFAB could help in this context, as its specifications would enable federated authentication for a variety of non-web protocols, thus gaining the benefits of federated authentication without any of the drawbacks that are currently experienced.

3.1.2. Cloud-Based Infrastructure Services

Typical IaaS or PaaS cloud use cases deal with provisioning on-demand cloud-based infrastructure services that may include infrastructure components such as computing and storage resources, network infrastructure, and other utilities. Cloud-based virtualized applications should ideally operate in the same way as regular non-virtualized applications whilst allowing management of the virtual computing resources (scaling, migration, reconfiguration) without changing the management applications.

In many cases, moving applications or platforms to the cloud may require their redesigning/refactoring to support dynamic deployment and configuration, including their security services, and authentication and authorization services. These will typically today be extensively based on manual setup and configuration of such components and features as trusted certificates and trust anchors, authorities and trusted services (both their location and certificates), attribute namespaces, and policies.

ABFAB could help in this context as a way of moving from the model of manually configured authentication and authorization towards a more easily managed system involving federated trust and identity, and ABFAB will be applicable for a wide range of existing features (e.g., connecting to a newly provisioned Virtual Machine through ABFAB-enabled Secure Shell (SSH) [RFC4251] instead of having to manually manage an administrative login to that machine).

3.2. High-Performance Computing

High-Performance Computing (HPC) is a discipline that uses supercomputers and computer clusters to solve complex computation problems; it is most commonly associated with scientific research or computational science.

Access to HPC resources, often mediated through technologies such as SSH, is typically managed through the use of user digital certificates [RFC5280] or through manually provisioned credentials and accounts. This requires HPC operators to issue certificates or accounts to users using a registration process that often duplicates identity management processes that already exist within most user organizations. The HPC community would like to utilize federated identity to perform both the user registration and authentication functions required to use HPC resources, and so reduce costs by avoiding this duplication of effort.

The HPC community also have the following additional requirements:

- Improve business continuity: In the event of operational issues at an HPC system at one organization (for example, a power failure), users and jobs could be transparently moved to other HPC systems without the overhead of having to manage user credentials for multiple organizations;

- Establish "HPC as a service": Many organizations who have invested in HPC systems want to make their systems easily available to external customers. Federated authentication facilitates this by enabling these customers to use their existing identity management, user credentialing, and support processes;

- Improve the user experience: Authentication to HPC systems is normally performed using user digital certificates, which some users find difficult to use. Federated authentication can provide a better user experience by allowing the use of other types of credentials, without requiring technical modifications to the HPC system to support these.

ABFAB could help in this context, as it could enable federated authentication for many of the protocols and technologies currently in use by HPC providers, such as SSH.

3.3. Grid Infrastructure

Grids are large-scale distributed infrastructures, consisting of many loosely coupled, independently managed, and geographically distributed resources managed by organizationally independent providers. Users of grids utilize these resources using grid middleware that allows them to submit and control computing jobs, manipulate datasets, communicate with other users, etc. These users are organized into Virtual Organizations (VOs); each VO represents a group of people working collaboratively on a common project. VOs facilitate both the management of their users and the meditation of agreements between their users and resource providers.

Authentication and authorization within most grids are performed using a Public Key Infrastructure, requiring each user to have an X.509 public-key certificate [RFC5280]. Authentication is performed through ownership of a particular certificate, while authorization decisions are made based on the user's identity (derived from their X.509 certificate), membership of a particular VO, or additional information assigned to a user by a VO. While efficient and scalable, this approach has been found wanting in terms of usability -- many users find certificates difficult to manage, for various reasons.

One approach to ameliorating this issue, adopted to some extent by some grid communities already, is to abstract away direct access to certificates from users, instead using alternative authentication mechanisms and then converting the credential provided by these into standard grid certificates. Some implementations of this idea use existing federated authentication techniques. However, current implementations of this approach suffer from a number of problems, not the least of which is the inability to use the federated credentials used to authenticate to a credential-conversion portal to also directly authenticate to non-web resources such as SSH daemons.

The ability to use federated authentication directly through ABFAB, without the use of a credential-conversion service, would allow users to authenticate to a grid and its associated services, allowing them to directly launch and control computing jobs, all without having to manage, or even see, an X.509 public-key certificate at any point in the process. Authorization within the grid would still be performed using VO membership as asserted by the user's Identity Provider (IdP) through the federated transport.

3.4. Databases and Directories

Databases (e.g., MySQL, PostgreSQL, Oracle) and directory technologies (e.g., OpenLDAP (http://www.openldap.org/), Microsoft Active Directory, Novell eDirectory) are very commonly used within many organizations for a variety of purposes. Such purposes can include core administrative functions, such as hosting identity information for its users, as well as business functions (e.g., student records systems at educational organizations).

Access to such database and directory systems is usually provided for internal users only; however, users external to the organizations sometimes require access to these systems directly -- for example, external examiners in educational organizations requiring access to student records systems, members of cross-organizational project teams who store information in a particular organization's systems, and external auditors.

Credentials for users either internal or external to the organization that allow access to these databases and directories are usually provisioned manually within an organization, either using identity management technologies or through more manual processes. For the internal users, this situation is fine -- this is one of the mainstays of identity management. However, for external users who require access, this represents more of a problem for organizational processes. The organization has to either (1) add these external users to its internal identity management systems or (2) provision these credentials directly within the database/directory systems and continue to manage them, including appropriate access controls associated with each credential, for the lifetime of that credential.

Federated authentication to databases or directories, via ABFAB technologies, would improve upon this situation, as it would remove the need to provision and de-provision credentials to access these systems. Organizations may still wish to manually manage access control of federated identities; however, even this could be provided through federated means, if the trust relationship between organizations was strong enough for the organization providing the service to rely upon it for this purpose.

3.5. Media Streaming

Media streaming services (audio or audio/video) are often provided publicly to anonymous users, but authentication is important for a protected subset of streams where rights management and access control must be applied.

Streams can be delivered via protocols that already include authentication, such as the Real Time Streaming Protocol (RTSP) [RFC2326] or RTP [RFC3550], or can be published in an encrypted form with keys only being distributed to trusted users. Federated authentication is applicable to both of these cases.

Alternative mechanisms to managing access exist -- for example, an approach where a unique stream URI is minted for each user. However, this relies on preserving the secrecy of the stream URI and also requires a communication channel between the web page used for authentication and the streaming service itself. Federated authentication would be a better fit for this kind of access control. Thus, ABFAB technologies that allow federated authentication directly within (inherently non-web) media streaming protocols would represent an enhancement to this area.

3.6. Printing

A visitor from one organization to the premises of another often requires the use of print services. Their home organization may of course offer printing, but the output could be a long way away, so the home service is not useful. The user will typically want to print from within a desktop or mobile application.

Where this service is currently offered, it would usually be achieved through the use of "open" printers (i.e., printers that allow anonymous print requests), where printer availability is advertised through the use of Bonjour or other similar protocols. If the organization requires authenticated print requests (usually for accounting purposes), the visitor would usually have to be given credentials that allow this, often supplemented with pay-as-you-go style payment systems.

Adding federated authentication to the Internet Printing Protocol (IPP) [RFC2911] (and other relevant protocols) would enable this kind of remote printing service without the administrative overhead of credentialing these visitors (who, of course, may well be one-time visitors to the organization). This would be immediately applicable to higher education, where this use case is increasingly important thanks to the success of federated network authentication systems such as eduroam (https://www.eduroam.org), but could also be used in other contexts such as commercial print kiosks, or in large heterogeneous organizations.

3.7. Accessing Applications from Devices on a Telecoms Infrastructure

Telecom operators typically have the following properties:

- A large collection of registered users, many of whom may have identities registered to a fairly high level of assurance (often for payment purposes). However, not all users will have this property -- for example, non-contract customers on mobile telecoms infrastructures in countries with low levels of identity registration requirements.

- An existing network infrastructure capable of authenticating a device (e.g., a cellphone or an Asymmetric Digital Subscriber Line (ADSL) router) and, by inference, its owner.

- A large collection of applications (both web-based and non-web-based) that its users wish to access using their devices. These applications could be hosted by the telecom operator directly, or they could be any application or system on the internet -- for example, network messaging services, VoIP, or email.

At present, authentication to these applications will be typically configured manually by the user on the device (or on a different device connected to that device) by inputting their (usually pre-provisioned out of band) credentials for that application -- one per application.

The use of ABFAB technologies in this case, via a mechanism dubbed "federated cross-layer access" (see [FCLA]) would greatly enhance the user experience of using these applications through devices. Federated cross-layer access would make use of the initial mutual authentication between device and network, to allow subsequent authentication and authorization to happen in a seamless manner for the user of that device authenticating to applications.

3.8. Enhanced Security Services for S/MIME

There are many situations where organizations want to protect information with robust access control, either for implementation of intellectual property right protections, for enforcement of contractual confidentiality agreements, or because of legal regulations. The Enhanced Security Services (ESS) for S/MIME defines an access control mechanism that is enforced by the recipient's client after decryption of the message (see [MSG-AC-REQ]). The data model used makes use of Policy Decision Points (PDPs), which make the policy decisions; Policy Enforcement Points (PEPs), which make decision requests to the PDP; and Policy Information Points (PIPs), which issue attributes about subjects. The decisions themselves are based on the policies and on the subject attributes.

The use of ABFAB technologies in this case would enable both the front-end and back-end attribute exchange required to provide subject attributes. When the PEP contacts the PDP, it would initiate an ABFAB authentication in order to authenticate to the PDP and allow it to obtain these required subject attributes. Once authenticated, the PDP would return a token to the subject PEP that could then be used for subsequent authentications to the PDP.

3.9. Smart Objects

Many smart device deployments involve multiple organizations that do not directly share security infrastructure. For example, in smart power deployments, devices (e.g., appliances) and infrastructure (e.g., electric car chargers) will wish to connect to an energy management system. The energy management system is provided by a utility company in some deployments. The utility company may wish to grant access only to authorized devices; for example, a consortium of utility companies and device manufacturers may certify devices to connect to power networks.

In another example, consumer devices may be used to access cloud services. For example, a camera could be bound to a photo processing site. Authentication and authorization for uploading pictures or ordering prints are required. Sensors could be used to provide data to services run by organizations other than the sensor manufacturer. Authorization and authentication can become very tricky when sensors have no user interface. Cellular devices may want to access services provided by a third party, regardless of whether the cellular network or Wi-Fi is used. This becomes difficult when authorization and billing are coordinated by the cellular provider.

The use of ABFAB technologies in this case would provide authentication between one entity, such as a smart device, and its IdP. Only two parties are involved in this exchange; this means that the smart device need not participate in any complicated public-key infrastructure even if it is authenticating against many cloud services. Instead, the device can delegate the process of authenticating the service, and even deciding whether the device should be permitted to access the service, to the IdP. This has several advantages. A wide variety of revenue-sharing models are enabled. Because device authentication is only with a single IdP, phishing of device credentials can be avoided. Authorization and decisions about what personal information to release are made by the IdP. The device owner can use a rich interface such as a website to configure authorization and privacy policy even if the device has no user interface. This model works well with pre-provisioning of device credentials.

4. Security Considerations

This document contains only use cases and defines no protocol operations for ABFAB. Security considerations for the ABFAB architecture are documented in [RFC7831], and security considerations for ABFAB technologies and protocols that are discussed in these use cases are documented in the corresponding protocol specifications.

5. References

5.1. Normative References

[RFC7831] Howlett, J., Hartman, S., Tschofenig, H., and J. Schaad, "Application Bridging for Federated Access Beyond Web (ABFAB) Architecture", RFC 7831, DOI 10.17487/RFC7831, May 2016, <http://www.rfc-editor.org/info/rfc7831>.

5.2. Informative References

[FCLA] Wei, Y., Ed., "Federated Cross-Layer Access", Work in Progress, draft-wei-abfab-fcla-02, March 2012.

[MSG-AC-REQ] Freeman, T., Schaad, J., and P. Patterson, "Requirements for Message Access Control", Work in Progress, draft-freeman-plasma-requirements-11, March 2015.

[OASIS.saml-profiles-2.0-os] Hughes, J., Cantor, S., Hodges, J., Hirsch, F., Mishra, P., Philpott, R., and E. Maler, "Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard OASIS.saml-profiles-2.0-os, March 2005, <http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>.

[RFC1939] Myers, J. and M. Rose, "Post Office Protocol - Version 3", STD 53, RFC 1939, DOI 10.17487/RFC1939, May 1996, <http://www.rfc-editor.org/info/rfc1939>.

[RFC2326] Schulzrinne, H., Rao, A., and R. Lanphier, "Real Time Streaming Protocol (RTSP)", RFC 2326, DOI 10.17487/RFC2326, April 1998, <http://www.rfc-editor.org/info/rfc2326>.

[RFC2911] Hastings, T., Ed., Herriot, R., deBry, R., Isaacson, S., and P. Powell, "Internet Printing Protocol/1.1: Model and Semantics", RFC 2911, DOI 10.17487/RFC2911, September 2000, <http://www.rfc-editor.org/info/rfc2911>.

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, DOI 10.17487/RFC3501, March 2003, <http://www.rfc-editor.org/info/rfc3501>.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, DOI 10.17487/RFC3550, July 2003, <http://www.rfc-editor.org/info/rfc3550>.

[RFC4251] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Architecture", RFC 4251, DOI 10.17487/RFC4251, January 2006, <http://www.rfc-editor.org/info/rfc4251>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <http://www.rfc-editor.org/info/rfc5321>.

Acknowledgments

These use cases have been developed and documented using significant input from Jens Jensen (STFC Rutherford Appleton Laboratory), Daniel Kouril (CESNET), Michal Prochazka (CESNET), Ian Stewart (University of Edinburgh), Stephen Booth (Edinburgh Parallel Computing Centre), Eefje van der Harst (SURFnet), Joost van Dijk (SURFnet), Robin Breathe (Oxford Brookes University), Yinxing Wei (ZTE Corporation), Trevor Freeman (Microsoft Corporation), Sam Hartman (Painless Security, LLC), and Yuri Demchenko (University of Amsterdam).

Contributors

The following individuals made important contributions to the text of this document: Tim Bannister (Manchester University), Simon Cooper (Jisc), Josh Howlett (Jisc), and Mark Tysom (Jisc).

Author's Address

Dr. Rhys Smith (editor)
Jisc
Lumen House, Library Avenue, Harwell
Oxford OX11 0SG
United Kingdom

Phone: +44 1235 822145
Email: rhys.smith@jisc.ac.uk