Unlocking data: federated identity with LSDMA and dCache

2015 J. Phys.: Conf. Ser. 664 042037

(http://iopscience.iop.org/1742-6596/664/4/042037)

Journal of Physics: Conference Series **664** (2015) 042037 doi:10.1088/1742-6596/664/4/042037

Unlocking data: federated identity with LSDMA and dCache

AP Millar[1], G Behrmann[2], C Bernardt[1], P Fuhrmann[1], M Hardt[3], A Hayrapetyan[3], D Litvintsev[4], T Mkrtchyan[1], A Rossi[4], K Schwank[1]

[1] IT Dept., DESY, Notkestrasse 85, Hamburg, Germany
[2] Gerd Behrmann, Copenhagen, Denmark
[3] Steinbuch Centre for Computing, Hermann-von-Helmholtz-Platz 1, Karlsruhe, Germany
[4] Fermilab, Batavia, IL, USA

E-mail: paul.millar@desy.de

Abstract. X.509, the dominant identity system from grid computing, has proved unpopular for many user communities. More popular alternatives generally assume the user is interacting via their web-browser. Such alternatives allow a user to authenticate with many services with the same credentials (user-name and password). They also allow users from different organisations form collaborations quickly and simply.

Scientists generally require that their custom analysis software has direct access to the data. Such direct access is not currently supported by alternatives to X.509, as they require the use of a web-browser.

Various approaches to solve this issue are being investigated as part of the Large Scale Data Management and Analysis (LSDMA) project, a German funded national R&D project. These involve dynamic credential translation (creating an X.509 credential) to allow backwards compatibility in addition to direct SAML- and OpenID Connect-based authentication.

We present a summary of the current state of art and the current status of the federated identity work funded by the LSDMA project along with the future road map.

1. Introduction

With the advent of the Large Hadron Collider (LHC) facility at CERN and the corresponding world-wide grid infrastructure, the World-wide LHC Computational Grid (WLCG), deploying and managing data that is spread across the globe became a reality. The community of scientists that need to access this data is equally distributed, requiring a common, decentralised authentication mechanism.

The adopted solution was X.509-based authentication. Users are issued with an X.509 certificate by their local certificate authority (CA), which typically operate nationally. The sites in WLCG that provide resources trust CAs through their membership of a global trust federation: the IGTF. By trusting these CAs, services can trust that the X.509 certificates they issue correctly identify the users.

Group-membership is an example of a service that authenticates via X.509 certificate. The user contacts the service, typically once per day, to receive a signed assertion (in the form of an additional X.509 certificate) which describes in which groups the user is a member. Later, when authenticating with other grid services, the user provides both their identity and their

group-membership assertion to the service. This allows the service to authorise the user based on their group-membership, rather than their individual identity.

The adoption of X.509 client certificates led to a world-wide, decentralised network of resources for the analysis and storage of LHC data. This model has spread, as the technology brought into production to support LHC use-cases is adapted to support other communities. However, X.509 client certificates remain a burden for users: it is neither a technology they are used to, nor something that existing software provides a good user experience. The extent to which this affects scientists is not to be understated: it is only the larger user communities that have adopted X.509 client certificates as their authentication mechanism as they have the resources to train their users in a new authentication mechanism. The result is that smaller communities are unable to access such resources.

Given the difficulties faced with X.509-based authentication, several projects have looked into providing a decentralised (or "federated") authentication mechanisms as alternatives. Security Assertion Markup Language (SAML) is perhaps the most widely deployed in academic environments. SAML allows the service to delegate responsibility for authenticating the user to another service. When the user successfully authenticates, the service receives an assertion describing that user.

2. Trust

Part of the problem faced by new users is in acquiring an X.509 certificate. In part, this is because membership of the IGTF requires the CA vets the user's identity with a face-to-face meeting and a state-issued identity card or passport. For new communities, this process is hard as they often have no access to an IGTF-accredited CA and establishing a new CA is prohibitively expensive.

This overhead is often unnecessary as the user's home institute (university or research facility) may have already vetted the user's identity with the level of scrutiny required by IGTF. Several services exist[1][2][3] that allow a user to acquire an X.509 user certificate in their web-browser based on this scrutiny. Typically SAML is used to allow the user to authenticate with their home institute and the service will accept the SAML assertion and provide the user with an X.509 certificate. Such services can provide the user with either provide long-lived (MICS profile) or short-lived (SLCS profile) certificates, depending on the intended use.

While this is an improvement, it carries two disadvantages: first, the use of SAML currently requires the use of a web-browser; second, the user is exposed to X.509 certificates, which generally require the user to gain experience using specialist software.

The requirement to use a web-browser comes from SAML and how it is commonly deployed. Currently, the authentication service run by the home institute and known as the identity provider (IdP), only support the user contacting it with a web-browser. The authentication challenge is an HTML web-page, typically requesting the user's user-name and password. Such a web-page is free-form and there is no practical way to automate this process. An alternative SAML-based authentication mechanism, called Enhanced Client or Proxy (ECP) profile, allows for an automated login; however, there are currently very few IdPs that support this profile, making it difficult to base a service on ECP. Without IdPs that support the ECP profile, it is difficult to use SAML outside of the web-browser.

3. Portals and delegation

One solution is to provide the users with a web-based front-end (portal) to mediate their computation and storage interactions. Such a portal acts as a graphical user interface (GUI) with which the user can steer their analysis and data-management activity. Once the user authenticates with the portal using SAML Web-SSO, the portal uses the SAML assertion to obtain an X.509 credential for that user. It then uses that credential when authenticating and

interacting with grid services on behalf of that user. This has the benefit of "hiding" the X.509 credential from the user, while still allowing that user to interact with grid services.

The other benefit from portal delegation is that all grid services that require X.509 based authentication may be used by someone who authenticates via SAML. There is no requirement for services to be updated. This is necessary as upgrading the hundred of sites that provide resources to WLCG is unfeasible.

To achieve this, the portal must obtain an X.509 credential representing the user. It is unpractical for the portal to run its own CA as setting up a CA, running it, and gaining IGTF accreditation is prohibitively expensive. Therefore, it useful to acquire a credential from some existing CA that supports the SLCS profile and which is already accredited within the IGTF. In Germany, the DFN already provides such a service, but it is targeted at providing certificates for users with web-browsers. A custom API is available for portal delegation, but this is not supported by existing portals. Therefore, an protocol translation service is needed between DFN-AAI and the existing portals.

4. Non-browser based approaches

When handling a much smaller set of resources, the restriction to continue using X.509 credentials may be lifted. For example, it is feasible for a site to update the service it provides to accept direct SAML-based authentication. If the user's software can obtain a SAML assertion then such an approach would allow the user to present this SAML assertion when authenticating.

A web service may be provided that allows a user to download the SAML assertion. If this is stored in a standard location then client software can locate and use it when authenticating. While not ideal, this provides a functional work-around to IdPs that support only Web-SSO and not ECP.

With the SAML assertion saved in the user's local machine, it becomes feasible to send the assertion as part of the login process. Software has been developed that can accept the SAML assertion as part of an LDAP login process. Since most server software can authenticate against an LDAP service, this allows users to authenticate to these services using their SAML assertion, provided the client software accepts the SAML assertion as the password.

Another non-browser SAML approach is to use ECP and a SLCS profile CA. In this approach, both the SLCS profile CA and the user's IdP support ECP. The client uses ECP to authenticate to the CA, which provides the client with a short-lived X.509 certificate. With this X.509 certificate, the client can interact with grid resources using the X.509 credential.

While a wide-spread deployment of this solution is unfeasible due to the lack of IdPs providing ECP support, for targeted groups with good contact with their IdP, this becomes feasible.

5. The work within LSDMA

LSDMA[4] (Large Scale Data Management and Analysis) is a project funded by the German government to link research of the Helmholtz Association of research centres in Germany with community specific Data Life Cycle Laboratories (DLCL). The DLCLs work in close cooperation with scientists and they process, manage and analyse data during its whole life cycle. The joint research and development activities in the DLCLs lead to community-specific tools and mechanisms. The DLCLs are complemented with a Data Services Integration Team (DSIT). This provides generic technologies and infrastructures for multi-community use, based on research and development in the areas of data management, data access and security, storage technologies and data preservation.

The dCache team at DESY and the group at KIT, as major partners within the LSDMA DSIT team, are working on solving these authentication problems through authenticating via SAML.

Within DSIT, the plan is to establish a federation of Identity Providers (IdPs) for Germany: LSDMA-AAI. This federation is similar to the existing DFN federation (DFN-AAI)[5] and we anticipate LSDMA-AAI becoming part of DFN-AAI in the future. The initial work will be on providing web-portals that allow a user to authenticate via SAML. An X.509 credential is built from that information, which is used when authenticating with data servers. This follows existing work in this direction[6].

Group-membership is a common concern across many projects as often it is desired to authorise some operation based on that user's group membership. A common group-membership service will be run within Germany to allow services to discover group membership of a user.

Current work involves establishing a credential-delegation service that allows a portal to request an X.509 credential and the DFN-AAI will mint an X.509 credential based on the user's SAML assertion, in turn provided by Web-SSO. This will enable portal delegation to work with IdPs in Germany.

In parallel, work is underway in providing a service that allows users to download their SAML assertion. When a user then saves their assertion, client software can use this when authenticating.

Yet another activity involves building clients that make use of ECP and coordinating effort in enabling ECP in both IdPs and the DFN-AAI SLCS CA service.

The final area of work is in enabling direct SAML-based authentication. This is either by embedding the assertion in the password field with the LDAP facade, or by updating support in the transfer protocols (e.g., FTP and NFS) to allow SAML-based authentication.

The ultimate goal is to allow scientists to access their data and to log into compute resources based solely on their home institute's assertion of their identity.

6. Conclusion

We have discussed some of the issues surrounding authentication; in particular, how the existing X.509-based grid infrastructure may be used by a user who authenticates via SAML Web-SSO. We also discussed ways in which infrastructure may be updated to support direct SAML-based authentication.

While considerable work remains, there are considerable benefits from allowing users to authenticate via their home institute. Reducing barriers and making it easier to access computing and storage resources will empower scientists in many disciplines to maximise the scientific output from the available data by maximising the utility of available resources.

Acknowledgments

Work described in this paper was funded by the LSDMA project, DESY, Fermilab and NDGF.

References

[1] Basney J, Fleury T and Gaynor J 2014 *Concurrency Computat.: Pract. Exper.* **26**(13) 2225–2239
[2] `http://www.terena.org/activities/tcs/`
[3] `https://www.aai.dfn.de/`
[4] van Wezel J, Streit A, Jung C, Stotzka R, Halstenberg S, Rigoll F, Garcia A, Heiss A, Schwarz K, Gasthuber M *et al.* 2012 *arXiv preprint arXiv:1212.5596*
[5] DFN-AAI website `https://www.aai.dfn.de/` accessed: 2014-1-20
[6] Groeper R, Grimm C, Piger S and Wiebelitz J 2007 *Software Engineering and Advanced Applications, 2007. 33rd EUROMICRO Conference on* (IEEE) pp 367–374