PSC Impact Analysis: Globus Toolkit Retirement

July 27, 2017 - Derek Simmel <dsimmel@psc.edu>

As posted at: https://github.com/globus/globus-toolkit/blob/globus_6_branch/support-changes.md, the Globus team has announced that support for the Globus Toolkit will be retired in January 2018, with only essential security updates to be applied until December 2018. The Globus team recommends that users migrate to their subscription-based Globus Cloud product line to replace software and services provided in the Globus Toolkit. Several meetings were held at the PEARC17 conference to discuss the impact of this announcement on various stakeholders, including relying parties in XSEDE, EGI, OSG and WLCG. This document describes the impact of the Globus Toolkit retirement on the services, operations and users of systems at the Pittsburgh Supercomputing Center (PSC).

Globus Toolkit

The Globus Toolkit (v.6) currently includes services, client applications, and libraries to facilitate X.509v3 credential issuance (e.g. MyProxy), job submission via Globus GRAM gateways, file transfer using the GridFTP protocol, and OpenSSH with Grid Security Infrastructure (GSI) authentication utilizing X.509v3 certificates. Third-party tools that work with Globus services (e.g., UberFTP) also rely on the GSI libraries for service and user authentication.

GSI-based user authentication

GSI authentication in services provided by the Globus Toolkit (GRAM, GridFTP, GSI-OpenSSH) employs (RSA) host keys and corresponding X.509v3 host certificates to authenticate client connections to services and to establish encrypted TLS sessions between clients and services and between pairs of distributed services (e.g., GridFTP servers). Users authenticate to these services using (RSA) keys and corresponding X.509v3 user certificates. Every server that runs a GSI-authenticated service (GRAM, GridFTP, GSI-OpenSSH) must have a host key and corresponding host certificate. In the XSEDE context, host and user certificates must, by policy, be issued by an IGTF-accredited certificate authority (CA) [see *Interoperable Global Trust Federation* below].

Upon successful user authentication using an X.509v3 user certificate, Globus Toolkit services (GridFTP, GSI-OpenSSH) perform a mapping from that user certificate subject (a.k.a. Distinguished Name or DN: a unique string in the certificate identifying the user) to that user's account name on the server. Mappings for all authorized users are maintained in a text file on the server, typically at `/etc/grid-security/grid-mapfile`. This file must be kept up-to-date by the server operators. PSC updates these files hourly via cron, drawing on data queried from the XSEDE central database and PSC site databases containing known user certificate subject strings from accepted CAs. This includes data received by PSC for XSEDE users via the XSEDE AMIE account provisioning services.

Upon retirement of services employing GSI-based user authentication, PSC as an XSEDE SP will need to implement new means to map XSEDE users to their PSC-local accounts for all services that allow users to authenticate using their federated XSEDE user identity (currently represented by their XSEDE User Portal username and password). These include Globus GRAM job submission, Globus GridFTP, and GSI-OpenSSH services.

PSC currently operates GSI-OpenSSH as one of two SSH services on Bridges login and data transfer nodes (DTNs). PSC also operates Globus GridFTP services on Bridges DTNs, DSC DTNs, and several data transfer test systems. All Globus GRAM services have been retired at PSC and are no longer operating.

All command-line clients used to obtain X.509v3 user certificates (e.g., `grid-proxy-init`, `myproxy-logon`) and GSI-based clients (e.g., `gsissh`, `gsiscp`, `gsisftp`, `globus-url-copy`, `globus-job-run`) will need to be retired and/or replaced with alternative tools and methods to provide equivalent functionality. Science gateways and 3rd-party services integrated with Globus Toolkit services (e.g. HTCondor) will also need to implement alternate means to retain current functionality.

Globus Cloud Services

As described in the Globus *support-changes.md* document, the Globus team recommends that current Globus Toolkit service operators migrate to the subscription-based Globus Cloud services, which includes Globus Connect file transfer services, and a new cloud-based user authentication service, Globus Auth. Subscription prices are negotiated directly with the Globus team, based on services and capabilities desired. Users who wish to use the web-based Globus transfer service between their own workstation and other Globus subscribers' endpoints may do so with a Basic (currently free) subscription.

XSEDE currently has a subscription to the Globus Cloud service. The extent to which XSEDE's Globus Cloud subscription sufficiently covers XSEDE SP site needs for access to Globus Cloud software and services is not entirely clear. Our current understanding is that XSEDE will continue to package and provide Globus software via the XSEDE Community Software Repository. We assume thereby that PSC should not need its own subscription to Globus Cloud services to deploy and operate XSEDE-provided Globus Cloud packages and services.

If PSC needs to operate Globus Cloud services for non-XSEDE systems and users, then PSC will need to pay for its own subscription to Globus Cloud services, since each service deployed must be registered separately with the Globus Cloud to function with the new cloud-based Globus Auth authentication framework.

XSEDE has already integrated authentication for the XSEDE User Portal with the Globus Auth service. This integration does not automatically extend to XSEDE SP sites and services. Each XSEDE SP, including PSC, will need to deploy new services and user authentication infrastructure to enable user authentication using Globus Auth.

Globus Auth

Globus Auth is a new cloud-based framework for user authentication, based on the OAuth 2.0 standard protocols (See https://docs.globus.org/api/auth/). As a replacement for GSI-based authentication, authentication with Globus Auth removes the need for users to obtain and manage keys and certificates. Users authenticate instead to the Globus Auth cloud service using either a Globus identity or a Globus-accepted federated identity (e.g., XSEDE, InCommon). XSEDE SP and PSC-deployed services integrated with Globus Auth will authenticate user access via OAuth 2.0 protocols.

It is not yet clear what assurance of user identity and authentication can be relied upon by PSC services integrated in future with Globus Auth. PSC will need to establish in writing the requirements and auditing means for user identity vetting, authentication and authorization for services relying on Globus Auth for user authentication. PSC will need to implement means to monitor and limit user access to services using Globus Auth-based authentication to comply with PSC policies and regulations. This includes vetting of users and community account connections arriving at PSC-hosted services via Science Gateways and other intermediate login services (e.g., XSEDE SSOHub) that will be integrated with Globus Auth.

Note that Globus Auth does not currently remove the need for PSC to obtain X.509v3 *host* certificates to operate Globus-related services. Host certificates remain necessary to authenticate connections to the services and to facilitate TLS encryption of sessions established between clients and Globus services operated on SP systems.

As stated in the *support-changes.md* document, the Globus team plans to provide a Globus Auth authentication mechanism for OpenSSH, implemented as a Linux Pluggable Authentication Modules (PAM) module, but this module is not yet available for testing. The PAM module approach is preferable to customization of the OpenSSH package itself (as was necessary for GSI-OpenSSH). Nevertheless, patching of OpenSSH will remain necessary to (1) include PSC's HPN-SSH data transfer performance enhancements, and (2) the `PermitPAMUserChange` SSH server configuration option included in GSI-OpenSSH to allow mapping from a federated identity to a site-local identity during OpenSSH PAM processing.

PSC MyProxy CA

PSC operates the IGTF-accredited PSC MyProxy CA on behalf of XSEDE as a secondary CA for short-term user certificate issuance. The deployment of this service includes two physical Linux servers, each of which has a Thales nShield Solo F2 500+ PCI Express hardware security module for secure CA key storage and hardware-acceleration of cryptographic functions (primarily digital signature generation). Annual service and software support cost for the Thales nShield modules is $763/module (total $1526). The MyProxy software, originally developed and maintained by NCSA, is currently provided and maintained as part of the Globus Toolkit distribution.

In an environment without GSI for authentication and which no longer relies on the PSC MyProxy CA to generate user certificates for user authentication, the PSC MyProxy CA may be retired and removed from service for XSEDE.

Impact on EGI, OSG and WLCG communities

The European Grid Infrastructure (EGI), Open Science Grid (OSG), and Worldwide Large Hadron Collider Grid (WLCG) communities have invested heavily in Globus and GSI-authenticated services in the past. During a meeting among Globus Toolkit stakeholders held at the PEARC17 conference, representatives of these large communities expressed their need and intent to continue supporting the current Globus Toolkit for their constituents for as long as needed until alternative replacements for the Globus Toolkit services and GSI authentication framework have been deployed and integrated into their communities' cyberinfrastructures.

In a statement entitled, "OSG Support of the Globus Toolkit" (June 6, 2017, https://opensciencegrid.github.io/technology/policy/globus-toolkit/), the OSG has stated that "OSG support for the Globus Toolkit (e.g., GridFTP and GSI) will continue for as long as stakeholders need it. Period. … When a software component reaches end-of-life, the OSG assists its stakeholders in managing the transition to new software to replace or extend those capabilities. … During such transition periods, OSG takes on traditional maintenance duties (i.e., patching, bug fixes and support) of the end-of-life software. The OSG is committed to keep the software secure until its stakeholders have successfully transitioned to new software."

Interoperable Global Trust Federation (IGTF)

Established in 2005, the IGTF (www.igtf.net) is an international standards body and trust federation serving worldwide distributed cyberinfrastructure for research. IGTF is comprised by three regional policy management authorities (PMAs): The Americas Grid PMA (TAGPMA), covering countries in North, Central, and South America and the Caribbean, the European Grid PMA (EUGridPMA), covering countries in Europe, Africa and the Middle East, and the Asia-Pacific Grid PMA (APGridPMA), covering countries from India to Japan, the South China Sea region and South Pacific including Australia and New Zealand. PSC staff member Derek Simmel has served as Chair of TAGPMA since 2011. PSC staff member Jim Marsteller serves as XSEDE representative in TAGPMA.

IGTF PMAs accredit certificate authorities (CAs) within their regions based on established international and IGTF standards and policies. IGTF maintains a distribution of trust anchors (CA certificates and associated data) for IGTF-accredited CAs. IGTF has also defined assurance profiles for user and service credentials, and is active in establishing standards for interoperation among identity federations and secure operations and communications for identity and authentication providers.

XSEDE is a Relying Party (RP) member of IGTF. XSEDE publishes a subset of the IGTF trust anchor distribution, representing the list of XSEDE-accepted CAs for host certificates and user certificates employed for service and user authentication and session security. The list of XSEDE-approved CAs currently includes:

```
/C=ch/O=CERN/CN=CERN Root Certification Authority 2
/C=DE/O=DFN-Verein/OU=DFN-PKI/CN=DFN-Verein PCA Grid - G01
/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Certification Authority
/C=IT/O=INFN/CN=INFN Certification Authority
/C=JP/O=KEK/OU=CRC/CN=KEK GRID Certificate Authority
/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
/C=UK/O=eScienceCA/OU=Authority/CN=UK e-Science CA 2B
/C=UK/O=eScienceRoot/OU=Authority/CN=UK e-Science Root
/C=US/O=DigiCert Grid/OU=www.digicert.com/CN=DigiCert Grid Trust CA
/C=US/O=DigiCert Grid/OU=www.digicert.com/CN=DigiCert Grid Trust CA G2
/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Assured ID Root CA
/C=US/O=Internet2/OU=InCommon/CN=InCommon IGTF Server CA
/C=US/O=National Center for Supercomputing Applications/OU=Certificate Authorities/CN=MyProxy CA 2013
/C=US/O=National Center for Supercomputing Applications/OU=Certificate Authorities/CN=Two Factor CA 2013
/C=US/O=Pittsburgh Supercomputing Center/CN=PSC MyProxy CA
/DC=ch/DC=cern/CN=CERN Grid Certification Authority
/DC=com/DC=DigiCert-Grid/O=DigiCert Grid/CN=DigiCert Grid CA-1
/DC=com/DC=DigiCert-Grid/O=DigiCert Grid/CN=DigiCert Grid Root CA
/DC=es/DC=irisgrid/CN=IRISGridCA
/DC=net/DC=ES/OU=Certificate Authorities/CN=NERSC Online CA
/DC=org/DC=cilogon/C=US/O=CILogon/CN=CILogon Basic CA 1
/DC=org/DC=cilogon/C=US/O=CILogon/CN=CILogon OSG CA 1
/DC=org/DC=cilogon/C=US/O=CILogon/CN=CILogon Silver CA 1
```

Although the XSEDE MyProxy CA (operated by NCSA) and PSC MyProxy CA may no longer be needed to retrieve X.509v3 certificates for XSEDE user authentication to GSI-based services, other IGTF-accredited CAs (e.g., InCommon IGTF Server CA) remain essential to provide X.509v3 host certificates for Globus services at XSEDE SPs including PSC.

Access to IGTF-accredited CAs for user certificates will continue to be needed for interoperation with other remote services in the U.S. and abroad that require them for authentication. These include the CILogon-Basic, CILogon-Silver, and CILogon-OSG CAs.