



GridSite/gLite delegation service

X.509 Proxy Certificates (PC) were originally introduced by the Globus Project and have subsequently become central to the operation of international production Grids, such as the LHC Computing Grid and the EGEE project. A proxy certificate allows jobs or agents to prove that they are running on behalf of a particular user, and they are granted to jobs by some form of delegation procedure involving the creation and signing of a short-lived X.509 certificate.

To delegate a proxy **from a client to a service**, the service is contacted by the client, which asks for an X.509 certificate request. The service then generates an RSA public and private key pair, stores the private key and uses the public key as the basis of an X.509 certificate request. The service returns the certificate request to the client, which enforces any restrictions it places on values such as expiration time, and then signs the request using the client's own private key. The resulting X.509 PC is then sent to the service, which now possesses the corresponding private key, the PC itself and all of the X.509 certificates which prove the chain of trust back to a trusted Certification Authority.

GridSite adds support to Apache for the authentication of clients using an X.509 proxy with an HTTPS connection. Web services can then be written as CGI scripts or executables, and obtain the authentication information, including the certificate chain used, from the CGI environment variables.

The **GridSite Delegation Service** uses this environment and is written in C with the aid of standard toolkits. The gSOAP web services toolkit is used to convert between SOAP messages and C structures, and OpenSSL is used to examine X.509 certificates and generate private keys and certificate requests. All the additional utility functions which are required, including the storage of proxies, are part of the GridSite library, where they can be used by third-party authors (such as the EGEE/gLite job submission system) to add a delegation portType to their own web services.

The **htproxypu**t command uses the client side components of the GridSite library to delegate, query, delete or renew proxies held by a server on the user's behalf.

